

505P0372WOOD

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-330872
(P 2 0 0 0 - 3 3 0 8 7 2 A)
(43) 公開日 平成12年11月30日 (2000. 11. 30)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
G06F 12/14	320	G06F 12/14	320 B
G09C 1/00	660	G09C 1/00	660 A
			660 D
G10L 19/00		G10L 9/00	N
H04L 9/10		H04L 9/00	621 Z

審査請求 未請求 請求項の数18 O L (全35頁)

(21) 出願番号 特願2000-76391 (P 2000-76391)
(22) 出願日 平成12年3月14日 (2000. 3. 14)
(31) 優先権主張番号 特願平11-69152
(32) 優先日 平成11年3月15日 (1999. 3. 15)
(33) 優先権主張国 日本 (J P)

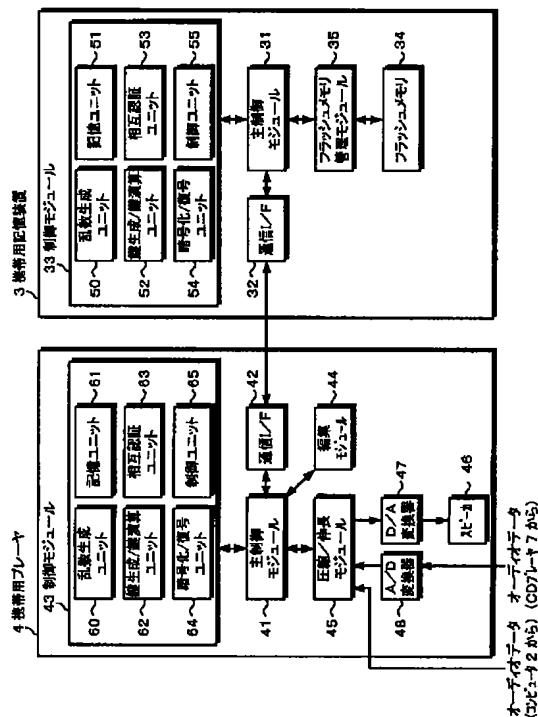
(71) 出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号
(72) 発明者 大石 丈於
東京都品川区北品川6丁目7番35号 ソニー株式会社内
(72) 発明者 岡上 拓己
東京都品川区北品川6丁目7番35号 ソニー株式会社内
(74) 代理人 100082762
弁理士 杉浦 正知

(54) 【発明の名称】 データ処理装置、データ処理システムおよびその方法

(57) 【要約】

【課題】 所定の処理ブロックを単位として圧縮などの処理されたデータを所定の暗号化ブロックを単位として暗号化して記憶媒体に記憶する際に、所定の処理ブロックに基づいた処理と復号処理とを簡単な構成で正確に行う。

【解決手段】 所定のデータ長の暗号化ブロックを単位としてデータを暗号化／復号ユニット64と、暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う圧縮／伸長モジュール45と、暗号化したデータを記憶するフラッシュメモリ34とを有し、携帯用プレーヤ4は、同じ暗号化ブロック内に位置するデータが同じ処理ブロック内に位置するように暗号化したデータをフラッシュメモリ34に書き込み、処理ブロックを単位としてデータをフラッシュメモリ34から読み出す。



【特許請求の範囲】

【請求項 1】 所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、
上記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、
上記暗号化したデータを記憶する記憶手段と、
同じ上記暗号化ブロック内に位置するデータが同じ上記処理ブロック内に位置するように、上記暗号化したデータを上記記憶手段に書き込み、上記処理ブロックを単位として上記データを上記記憶手段から読み出す制御手段とを有するデータ処理装置。

【請求項 2】 請求項 1 において、
上記制御手段は、上記処理ブロックにデータ長調整用のデータを入れて、上記処理ブロックのデータ長が上記暗号化ブロックのデータ長の整数倍になるように調整するデータ処理装置。

【請求項 3】 請求項 1 において、
上記暗号化手段は、上記暗号化を行おうとする上記暗号化ブロックと当該暗号化ブロックの直前の暗号化ブロックを暗号化して得た暗号文とを用いて演算を行い、当該演算の結果を暗号化するデータ処理装置。

【請求項 4】 請求項 1 において、
上記制御手段は、単数または複数の上記処理ブロックと、当該単数または複数の上記処理ブロックのうち最初に暗号化された上記処理ブロック内で最初に暗号化された上記暗号化ブロックを暗号化する際に用いられた初期値とを含むクラスタを用いて、上記記憶手段に記憶された上記暗号化されたデータを管理するデータ処理装置。

【請求項 5】 請求項 1 において、
上記制御手段は、単数または複数の上記処理ブロックを暗号化された順で上記記憶手段の連続したアドレスに記憶し、さらに、上記処理ブロック内の単数または複数の暗号化ブロックを暗号化された順で上記記憶手段の連続したアドレスに記憶し、上記クラスタ内で最初に暗号化された処理ブロック内でさらに最初に暗号化された暗号化ブロックが記憶された上記記憶手段のアドレスの直前のアドレスに上記初期値を記憶するデータ処理装置。

【請求項 6】 請求項 1 において、
上記制御手段は、上記処理ブロック単位で読み出した上記データを上記処理手段に出力するデータ処理装置。

【請求項 7】 請求項 1 において、
上記データは、圧縮されており、
上記処理手段は、上記記憶手段から読み出された上記データを、上記処理ブロックを単位として伸長するデータ処理装置。

【請求項 8】 記憶装置とデータ処理装置との間で相互認証を行いながらデータの入出力を行うデータ処理システムにおいて、
上記記憶装置は、

上記データ処理装置との間で相互認証処理を行う第 1 の相互認証処理手段と、

上記データを記憶する記憶手段と、

上記相互認証処理によって上記データ処理装置が正当な相手であると認めたときに、上記データ処理装置と上記記憶手段との間でデータの入出力を行わせる第 1 の制御手段とを有し、

上記データ処理装置は、

上記記憶装置との間で相互認証処理を行う第 2 の相互認証処理手段と、

所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、

上記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、

上記相互認証処理によって、上記記憶装置が正当な相手であると認めたときに、書き込み処理および読み出し処理の少なくとも一方を行い、上記書き込み処理において、同じ上記暗号化ブロック内に位置するデータが同じ上記処理ブロック内に位置するように、上記暗号化したデータを上記記憶手段に書き込み、上記読み出し処理において、上記処理ブロックを単位として上記データを上記記憶手段から読み出す制御手段とを有するデータ処理システム。

【請求項 9】 請求項 8 において、
上記第 2 の制御手段は、上記処理ブロックにデータ長調整用のデータを入れて、上記処理ブロックのデータ長が上記暗号化ブロックのデータ長の整数倍になるように調整するデータ処理システム。

【請求項 10】 請求項 8 において、
上記暗号化手段は、上記暗号化を行おうとする上記暗号化ブロックと当該暗号化ブロックの直前の暗号化ブロックを暗号化して得た暗号文とを用いて演算を行い、当該演算の結果を暗号化するデータ処理システム。

【請求項 11】 請求項 8 において、
上記第 2 の制御手段は、単数または複数の上記処理ブロックと、当該単数または複数の上記処理ブロックのうち最初に暗号化された上記処理ブロック内で最初に暗号化された上記暗号化ブロックを暗号化する際に用いられた初期値とを含むクラスタを用いて、上記記憶手段に記憶された上記暗号化されたデータを管理するデータ処理システム。

【請求項 12】 請求項 8 において、
上記第 2 の制御手段は、単数または複数の上記処理ブロックを暗号化された順で上記記憶手段の連続したアドレスに記憶し、さらに、上記処理ブロック内の単数または複数の暗号化ブロックを暗号化された順で上記記憶手段の連続したアドレスに記憶し、上記クラスタ内で最初に暗号化された処理ブロック内でさらに最初に暗号化された暗号化ブロックが記憶された上記記憶手段のアドレス

の直前のアドレスに上記初期値を記憶するデータ処理システム。

【請求項 1 3】 所定のデータ長の暗号化ブロックを単位としてデータを暗号化し、

上記暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行い、
同じ上記暗号化ブロック内に位置するデータが同じ上記処理ブロック内に位置するように、上記暗号化したデータを上記記憶手段に書き込み、上記処理ブロックを単位として上記データを上記記憶手段から読み出すデータ処理方法。

【請求項 1 4】 請求項 1 3 において、
上記処理ブロックにデータ長調整用のデータを入れて、
上記処理ブロックのデータ長が上記暗号化ブロックのデータ長の整数倍になるように調整するデータ処理方法。

【請求項 1 5】 請求項 1 3 において、
上記暗号化を行おうとする上記暗号化ブロックと当該暗号化ブロックの直前の暗号化ブロックを暗号化して得た暗号文とを用いて演算を行い、当該演算の結果を暗号化して上記暗号化を行うデータ処理方法。

【請求項 1 6】 請求項 1 3 において、
単数または複数の上記処理ブロックと、当該単数または複数の上記処理ブロックのうち最初に暗号化された上記処理ブロック内で最初に暗号化された上記暗号化ブロックを暗号化する際に用いられた初期値とを含むクラスタを用いて、記憶された上記暗号化されたデータを管理するデータ処理方法。

【請求項 1 7】 請求項 1 3 において、
単数または複数の上記処理ブロックを暗号化された順で記憶手段の連続したアドレスに記憶し、さらに、上記処理ブロック内の単数または複数の暗号化ブロックを暗号化された順で上記記憶手段の連続したアドレスに記憶し、上記クラスタ内で最初に暗号化された処理ブロック内でさらに最初に暗号化された暗号化ブロックが記憶された上記記憶手段のアドレスの直前のアドレスに上記初期値を記憶するデータ処理方法。

【請求項 1 8】 請求項 1 3 において、
読み出された上記データを、上記処理ブロックを単位として伸長するデータ処理方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】 この発明は、例えば圧縮などの所定の処理ブロックを単位で処理されたデータを所定の暗号化ブロックを単位として暗号化して記憶手段に記憶するデータ処理装置、データ処理手段およびその方法に関する。

【0 0 0 2】

【従来の技術】 例えば、著作権侵害となる不正利用を防止するために、オーディオデータなどのデータを所定のデータ長の暗号化ブロックを単位として暗号化して記憶

媒体に記憶することがある。この場合に、暗号化しようとするデータは、通常、所定の圧縮処理ブロックを単位として圧縮されていることが多い。

【0 0 0 3】

【発明が解決しようとする課題】 ところで、上述したように圧縮されたデータを暗号化して記憶媒体に記録する場合に、圧縮ブロックと暗号化ブロックと通常一致しない。そのため、例えば、圧縮ブロックを単位として記憶媒体からデータを読み出すと暗号化ブロックのうち一部のブロックのデータが読み出されないことがあり、正確な復号を行えなくなる。このような事態を回避するために、圧縮ブロックおよび暗号化ブロックの双方を考慮して読み出しを行うと、処理が煩雑となる問題がある。

【0 0 0 4】 また、記憶媒体に記録したデータを編集する場合などは、例えば圧縮ブロックを単位としてデータの分割および結合などが行われるが、この場合にも、編集後のデータに暗号化ブロックの一部のデータが含まなくなる可能性が高く、同様に、正確な復号が行えなくなるという問題がある。また、圧縮されていないデータであっても、例えば音楽用の CD (Compact Disc:登録商標) フォーマットなどのように、所定のブロックを単位として処理が行われる場合にも上述した場合と同様の問題が生じる。

【0 0 0 5】 この発明の目的は、上述した従来技術の問題点に鑑みてなされ、例えば圧縮などの所定の処理ブロック単位で処理されたデータを所定の暗号化ブロックを単位として暗号化して記憶媒体に記憶する際に、所定の処理ブロックに基づいた処理と復号処理とを簡単な構成で正確に行うことができるデータ処理装置、データ処理システムおよびその方法を提供することにある。

【0 0 0 6】

【課題を解決するための手段】 上述した課題を解決するために、請求項 1 の発明は、所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、暗号化したデータを記憶する記憶手段と、同じ暗号化ブロック内に位置するデータが同じ処理ブロック内に位置するように、暗号化したデータを記憶手段に書き込み、処理ブロックを単位としてデータを記憶手段から読み出す制御手段とを有するデータ処理装置である。

【0 0 0 7】 請求項 1 3 の発明は、所定のデータ長の暗号化ブロックを単位としてデータを暗号化し、暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行い、同じ暗号化ブロック内に位置するデータが同じ処理ブロック内に位置するように、暗号化したデータを記憶手段に書き込み、処理ブロックを単位としてデータを記憶手段から読み出すデータ処理方法である。

【 0 0 0 8 】請求項 8 の発明は、記憶装置とデータ処理装置との間で相互認証を行いながらデータの入出力を行うデータ処理システムにおいて、記憶装置は、データ処理装置との間で相互認証処理を行う第 1 の相互認証処理手段と、データを記憶する記憶手段と、相互認証処理によってデータ処理装置が正当な相手であると認めたときに、データ処理装置と記憶手段との間でデータの入出力を行わせる第 1 の制御手段とを有し、データ処理装置は、記憶装置との間で相互認証処理を行う第 2 の相互認証処理手段と、所定のデータ長の暗号化ブロックを単位としてデータを暗号化する暗号化手段と、暗号化ブロックの整数倍のデータ長を持つ処理ブロックを単位としてデータに所定の処理を行う処理手段と、相互認証処理によって、記憶装置が正当な相手であると認めたときに、書き込み処理および読み出し処理の少なくとも一方を行い、書き込み処理において、同じ暗号化ブロック内に位置するデータが同じ処理ブロック内に位置するように、暗号化したデータを記憶手段に書き込み、読み出し処理において、処理ブロックを単位としてデータを記憶手段から読み出す制御手段とを有するデータ処理システムである。

【 0 0 0 9 】

【発明の実施の形態】以下、この発明の実施形態に係わるオーディオシステムについて説明する。図 1 は、一実施形態のオーディオシステム 1 のシステム構成図、図 2 は図 1 に示す携帯用記憶装置 3 および携帯用プレーヤ 4 の内部構成図である。図 1 に示すように、オーディオシステム 1 は、例えば、コンピュータ 2、携帯用記憶装置 3、携帯用プレーヤ 4、CD-ROM ドライブ 6 および CD プレーヤ 7 を有する。

【 0 0 1 0 】コンピュータ 2

コンピュータ 2 は、ネットワーク 5 に接続されており、例えば、EMD (Electronic Music Distribution: 電子音楽配信) などのサービスを提供する図示しないサービスプロバイダのホストコンピュータから、ネットワーク 5 を介してオーディオデータ (トラックデータ) を受信し、当該受信したオーディオデータを必要に応じて復号して、携帯用プレーヤ 4 に出力する。また、コンピュータ 2 は、コンテンツデータを受信するに当たって、必要に応じて、サービスプロバイダのホストコンピュータとの間で認証処理および課金処理などを行う。また、コンピュータ 2 は、例えば、CD-ROM ドライブ 6 から入力したオーディオデータを携帯用プレーヤ 4 に出力する。

【 0 0 1 1 】携帯用記憶装置 3

携帯用記憶装置 3 は、携帯用プレーヤ 4 に対して着脱自在とされ、例えば、メモリスティック (Memory Stick: 商標) であり、フラッシュメモリなどの書き換え可能な半導体メモリを内蔵している。本明細書において、メモリカードの用語が使用されることもあるが、メモリカード

は、携帯用記憶装置を指すものとして使用している。図 2 に示すように、携帯用記憶装置 3 は、例えば、主制御モジュール 3 1、通信インターフェイス 3 2、制御モジュール 3 3、フラッシュメモリ 3 4 およびフラッシュメモリ管理モジュール 3 5 を有する。

【 0 0 1 2 】〔制御モジュール 3 3〕図 2 に示すように、制御モジュール 3 3 は、例えば、乱数発生ユニット 5 0、記憶ユニット 5 1、鍵生成/演算ユニット 5 2、相互認証ユニット 5 3、暗号化/復号ユニット 5 4 および制御ユニット 5 5 を有する。制御モジュール 3 3 は、シングルチップの暗号処理専用の集積回路であり、多層構造を有し、内部のメモリセルはアルミニウム層などのダミー層に挟まれている。また、制御モジュール 3 3 は、動作電圧または動作周波数の幅が狭く、外部から不正にデータを読み出せないように耐タンパー性を有している。乱数発生ユニット 5 0 は、乱数発生指示を受けると、64 ビット (8 バイト) の乱数を発生する。

【 0 0 1 3 】記憶ユニット 5 1 は、例えば、EEPROM (Electrically Erasable Programmable Read Only Memory) などの不揮発性メモリであり、認証処理に必要な鍵データなどの種々のデータを記憶している。図 3 は、記憶ユニット 5 1 に記憶されているデータを説明するための図である。図 3 に示すように、記憶ユニット 5 1 は、認証鍵データ $IK_0 \sim IK_{31}$ 、装置識別データ ID および記憶用鍵データ SK_0 を記憶している。

【 0 0 1 4 】認証鍵データ $IK_0 \sim IK_{31}$ は、携帯用記憶装置 3 が携帯用プレーヤ 4 との間で相互認証を行う際に用いられる鍵データであり、後述するように相互認証を行う度に認証鍵データ $IK_0 \sim IK_{31}$ のうちの認証鍵データがランダムに選択される。なお、認証鍵データ $IK_0 \sim IK_{31}$ および記憶用鍵データ SK_0 は、携帯用記憶装置 3 の外部から読めないようになっている。装置識別データ ID は、携帯用記憶装置 3 に対してユニークに付けられた識別データであり、後述するように、携帯用記憶装置 3 が携帯用プレーヤ 4 との間で相互認証を行う際に読み出されて携帯用プレーヤ 4 に出力される。記憶用鍵データ SK_0 は、後述するように、コンテンツ鍵データ CK を暗号化してフラッシュメモリ 3 4 に記憶する際に用いられる。

【 0 0 1 5 】鍵生成/演算ユニット 5 2 は、例えば、ISO/IEC 9797 の MAC (Message Authentication Code) 演算などの種々の演算を行って鍵データを生成する。このとき、MAC 演算には、例えば、"Block cipher Algorithm" として FIPS PUB 46-2 に規定される DES (Data Encryption Standard) が用いられる。MAC 演算は、任意の長さのデータを固定の長さに圧縮する一方向性ハッシュ関数演算であり、関数値が秘密鍵に依存して定まる。

【 0 0 1 6 】相互認証ユニット 5 3 は、携帯用プレーヤ 4 からオーディオデータを入力してフラッシュメモリ 3

4 に書き込む動作を行うのに先立って、携帯用プレーヤ 4 との間で相互認証処理を行う。また、相互認証ユニット 5 3 は、フラッシュメモリ 3 4 からオーディオデータを読み出して携帯用プレーヤ 4 に出力する動作を行うのに先立って、携帯用プレーヤ 4 との間で相互認証処理を行う。また、相互認証ユニット 5 3 は、相互認証処理において、前述した MAC 演算を行う。当該相互認証処理では、記憶ユニット 5 1 に記憶されているデータが用いられる。

【 0 0 1 7 】暗号化／復号ユニット 5 4 は、DES、IDEA、MISTY などのブロック暗号アルゴリズムでの暗号化を行う。使用するモードは、FIPS PUB 81" DES MODES OF OPERATION" に規定されているような ECB (Electronic Code Book) モードおよび CBC (Cipher Block Chaining) モードである。また、暗号化／復号ユニット 5 4 は、DES、IDEA、MISTY などのブロック復号アルゴリズムでの復号を行う。使用するモードは、上記 ECB モードおよび CBC モードである。当該 ECB モードおよび CBC モードのブロック暗号化／復号では、指定された鍵データを用いて指定されたデータを暗号化／復号する。制御ユニット 5 5 は、乱数発生ユニット 5 0、記憶ユニット 5 1、鍵生成／演算ユニット 5 2、相互認証ユニット 5 3 および暗号化／復号ユニット 5 4 の処理を統括して制御する。

【 0 0 1 8 】〔フラッシュメモリ 3 4〕フラッシュメモリ 3 4 は、例えば、3 2 M バイトの記憶容量を有する。フラッシュメモリ 3 4 には、相互認証ユニット 5 3 による相互認証処理によって正当な相手であると認められたときに、携帯用プレーヤ 4 から入力したオーディオデータが書き込まれる。また、フラッシュメモリ 3 4 からは、相互認証ユニット 5 3 による相互認証処理によって正当な相手であると認められたときに、オーディオデータが読み出されて携帯用プレーヤ 4 に出力される。

【 0 0 1 9 】以下、フラッシュメモリ 3 4 に記憶されるデータおよびそのフォーマットについて説明する。図 4 は、フラッシュメモリ 3 4 に記憶されるデータを説明するための図である。図 4 に示すように、フラッシュメモリ 3 4 には、例えば、再生管理ファイル 1 0 0、トラックデータファイル 1 0 1₀、1 0 1₁、1 0 1₂、1 0 1₃ が記憶されている。ここで、再生管理ファイル 1 0 0 はトラックデータファイル 1 0 1₀、1 0 1₁、1 0 1₂、1 0 1₃ の再生を管理する管理データを有し、トラックデータファイル 1 0 1₀、1 0 1₁、1 0 1₂、1 0 1₃ はそれぞれ対応するトラックデータ（オーディオデータ）を有している。なお、本実施形態では、トラックデータは、例えば、1 曲分のオーディオデータを意味する。

【 0 0 2 0 】図 5 は、再生管理ファイルの構成を示し、図 6 が一つ（1 曲）の ATRAC 3 データファイルの構成を示す。再生管理ファイルは、1 6 K B 固定長のファ

イルである。ATRAC 3 データファイルは、曲単位をもって、先頭の属性ヘッダと、それに続く実際の暗号化された音楽データとからなる。属性ヘッダも 1 6 K B 固定長とされ、再生管理ファイルと類似した構成を有する。

【 0 0 2 1 】再生管理ファイルは、ヘッダ、1 バイトコードのメモリカードの名前 NM 1 - S、2 バイトコードのメモリカードの名前 NM 2 - S、曲順の再生テーブル TRK TBL、メモリカード全体の付加情報 INF - S とからなる。データファイルの先頭の属性ヘッダは、ヘッダ、1 バイトコードの曲名 NM 1、2 バイトコードの曲名 NM 2、トラックのキー情報等のトラック情報 TRK INF、パーツ情報 PRT INF と、トラックの付加情報 INF とからなる。ヘッダには、総パーツ数、名前の属性、付加情報のサイズの情報等が含まれる。

【 0 0 2 2 】属性ヘッダに対して ATRAC 3 の音楽データが続く。音楽データは、1 6 K B のブロック毎に区切られ、各ブロックの先頭にヘッダが付加されている。ヘッダには、暗号を復号するための初期値が含まれる。なお、暗号化の処理を受けるのは、ATRAC 3 データファイル中の音楽データのみであって、それ以外の再生管理ファイル、ヘッダ等のデータは、暗号化されない。

【 0 0 2 3 】図 7 は、再生管理ファイル PBLIST のより詳細なデータ構成を示し、図 8 A、図 8 B は、再生管理ファイル PBLIST を構成するヘッダとそれ以外の部分をそれぞれ示す。再生管理ファイル PBLIST は、1 クラスタ（1 ブロック = 1 6 K B）のサイズである。ヘッダ（図 8 A）が 3 2 バイトである。ヘッダ以外の部分（図 8 B）がメモリカード全体に対する名前 NM 1 - S（2 5 6 バイト）、名前 NM 2 - S（5 1 2 バイト）、CONTENTS KEY、MAC、S - YMD hms と、再生順番を管理するテーブル TRK TBL（8 0 0 バイト）と、メモリカード全体に対する付加情報 INF - S（1 4 7 2 0 バイト）であり、最後にヘッダ中の情報の一部が再度記録される。これらの異なる種類のデータ群のそれぞれの先頭は、再生管理ファイル内で所定の位置となるように規定されている。

【 0 0 2 4 】再生管理ファイルは、（0 x 0 0 0 0）および（0 x 0 0 1 0）で表される先頭から 3 2 バイト（図 8 A）がヘッダである。なお、ファイル中で先頭から 1 6 バイト単位で区切られた単位をスロットと称する。ファイルの第 1 および第 2 のスロットに配されるヘッダには、下記の意味、機能、値を持つデータが先頭から順に配される。なお、Reserved と表記されているデータは、未定義のデータを表している。通常ヌル（0 x 0 0）が書かれるが、何が書かれていても Reserved のデータが無視される。将来のバージョンでは、変更がありうる。また、この部分への書き込みは禁止する。Option と書かれた部分も使用しない場合は、全て Reserved と同じ扱いとされる。

【0025】BLKID-TL0 (4バイト)

意味: BLOCKID FILE ID

機能: 再生管理ファイルの先頭であることを識別するための値

値: 固定値="TL=0" (例えば0x544C2D30)

MCODE (2バイト)

意味: MAKER CODE

機能: 記録した機器の、メーカー、モデルを識別するコード

値: 上位10ビット (メーカーコード) 下位6ビット (機種コード)

REVISION (4バイト)

意味: PBLISTの書き換え回数

機能: 再生管理ファイルを書き換える度にインクリメント

値: 0より始まり+1ずつ増加する

S-YMDhms (4バイト) (Option)

意味: 信頼できる時計を持つ機器で記録した年・月・日・時・分・秒

機能: 最終記録日時を識別するための値

値: 25~31ビット 年 0~99 (1980~2079)

21~24ビット 月 0~12

16~20ビット 日 0~31

11~15ビット 時 0~23

05~10ビット 分 0~59

00~04ビット 秒 0~29 (2秒単位)。

【0026】SN1C+L (2バイト)

意味: NM1-S領域に書かれるメモ리카ードの名前 (1バイト) の属性を表す

機能: 使用する文字コードと言語コードを各1バイトで表す

値: 文字コード (C) は上位1バイトで下記のように文字を区別する

00: 文字コードは設定しない。単なる2進数として扱うこと

01: ASCII 02: ASCII+KANA 03: modified8859-1

81: MS-JIS 82: KS C 5601-1989 83: GB2312-80 90: S-JIS (for Voice)。

【0027】言語コード (L) は下位1バイトで下記のようにEBU Tech 3258 規定に準じて言語を区別する

00: 設定しない 08: German 09: English 0A: Spanish

0F: French 15: Italian 1D: Dutch

65: Korean 69: Japanese 75: Chinese

データが無い場合オールゼロとすること。

【0028】SN2C+L (2バイト)

意味: NM2-S領域に書かれるメモ리카ードの名前 (2バイト) の属性を表す

機能: 使用する文字コードと言語コードを各1バイトで

表す

値: 上述したSN1C+Lと同一

SINF SIZE (2バイト)

意味: INF-S領域に書かれるメモ리카ード全体に関する付加情報の全てを合計したサイズを表す

機能: データサイズを16バイト単位の大きさを記述、無い場合は必ずオールゼロとすること

値: サイズは0x0001から0x39C (924)

T-TRK (2バイト)

10 意味: TOTAL TRACK NUMBER

機能: 総トラック数

値: 1から0x0190 (最大400トラック)、データが無い場合はオールゼロとすること

VerNo (2バイト)

意味: フォーマットのバージョン番号

機能: 上位がメジャーバージョン番号、下位がマイナーバージョン番号

値: 例 0x0100 (Ver1. 0)

0x0203 (Ver2. 3)。

20 【0029】上述したヘッダに続く領域に書かれるデータ (図8B) について以下に説明する。

【0030】NM1-S

意味: メモ리카ード全体に関する1バイトの名前

機能: 1バイトの文字コードで表した可変長の名前データ (最大で256)

名前データの終了は、必ず終端コード (0x00) を書き込むこと

サイズはこの終端コードから計算すること、データの無い場合は少なくとも先頭 (0x0020) からヌル (0x00) を1バイト以上記録すること

30

値: 各種文字コード

NM2-S

意味: メモ리카ード全体に関する2バイトの名前

機能: 2バイトの文字コードで表した可変長の名前データ (最大で512)

名前データの終了は、必ず終端コード (0x00) を書き込むこと

サイズはこの終端コードから計算すること、データの無い場合は少なくとも先頭 (0x0120) からヌル (0x00) を2バイト以上記録すること

40

値: 各種文字コード。

【0031】CONTENTS KEY

意味: 曲ごとに用意された値でMG (M) で保護されてから保存される。ここでは、1曲目に付けられるCONTENTS KEYと同じ値

機能: S-YMDhmsのMACの計算に必要な鍵となる

値: 0から0xFFFFFFFFFFFFFFFFFFFFFFFFまで

50 意味: 著作権情報改ざんチェック値

機能：S-YMDhmsの内容とCONTENTS KEYから作成される値

値：0から0xFFFFFFFFFFFFFFFFFまで。

【0 0 3 2】TRK-n n n

意味：再生するATRAC3データファイルのSQN
(シーケンス) 番号

機能：TRKINFの中のFN○を記述する

値：1から400 (0x190)

トラックが存在しない時はオールゼロとすること
I N F - S

意味：メモリカード全体に関する付加情報データ（例えば写真、歌詞、解説等の情報）

機能：ヘッダを伴った可変長の付加情報データ

複数の異なる付加情報が並べられることがある。それぞれに ID とデータサイズが付けられている。個々のヘッダを含む付加情報データは最小 16 バイト以上で 4 バイトの整数倍の単位で構成される。その詳細については、後述する

値：付加情報データ構成を参照

S - Y M D h m s (4 バイト) (O p t i o n)

意味：信頼できる時計を持つ機器で記録した年・月・日
・時・分・秒

機能：最終記録日時を識別するための値、EMDの時は必須

値：25～31ビット 年 0～99（1980～2079）

21～24ビット 月 0～12

16～20ビット 日 0～31

11~15ビット 時 0~23

05～10ビット 分 0～59

00～04ビット 秒 0～29（2秒単位）。

【0033】再生管理ファイルの最後のスロットとして、ヘッダ内のものと同一のBLKID-TL0と、MCodeと、REVISIONとが書かれる。

【0034】民生用オーディオ機器として、メモリカードが記録中に抜かれたり、電源が切れることがあり、復活した時にこれらの異常の発生を検出することが必要とされる。上述したように、REVISIONをブロックの先頭と末尾に書き込み、この値を書き換える度に+1インクリメントするようにしている。若し、ブロックの途中で異常終了が発生すると、先頭と末尾のREVISIONの値が一致せず、異常終了を検出することができる。REVISIONが2個存在するので、高い確率で異常終了を検出することができる。異常終了の検出時には、エラーメッセージの表示等の警告が発生する。

【0035】また、1ブロック（16KB）の先頭部分に固定値BLKID-TL0を挿入しているので、FATが壊れた場合の修復の目安に固定値を使用できる。すなわち、各ブロックの先頭の固定値を見れば、ファイル

の種類を判別することが可能である。しかも、この固定値BLKID-TL0は、ブロックのヘッダおよびブロックの終端部分に二重に記述するので、その信頼性のチェックを行うことができる。なお、再生管理ファイルPBLISTの同一のものを二重に記録しても良い。

【0036】ATRAC3データファイルは、トラック情報管理ファイルと比較して、相当大きなデータ量（例えば数千のブロックが繋がる場合もある）であり、ATRAC3データファイルに関しては、後述するように、ブロック番号BLOCK SERIALが付けられている。但し、ATRAC3データファイルは、通常複数のファイルがメモリカード上に存在するので、CONNUMでコンテンツの区別を付けた上で、BLOCK SERIALを付けないと、重複が発生し、FATが壊れた場合のファイルの復旧が困難となる。

【0037】同様に、FATの破壊までにはいたらないが、論理を間違ってファイルとして不都合のあるような場合に、書き込んだメーカーの機種が特定できるように、メーカーコード(MCode)がブロックの先頭と末尾に記録されている。

【0038】図8Cは、付加情報データの構成を示す。付加情報の先頭に下記のヘッダが書かれる。ヘッダ以降に可変長のデータが書かれる。

【0039】INF

意味: FIELD ID

機能：付加情報データの先頭を示す固定値

值：0 x 6 9

ID

意味：付加情報キーコード

30 機能：付加情報の分類を示す

値：0 から 0 x FF

SIZE

意味：個別の付加情報の大きさ

機能：データサイズは自由であるが、必ず4バイトの整数倍でなければならない。また、最小16バイト以上のこと。データの終わりより余りがでる場合はヌル(0x00)で埋めておくこと

値：16から14784 (0x39C0)

MC o d e

40 意味: MAKER CODE

機能：記録した機器の、メーカー、モデルを識別するコード

値：上位 10 ビット（メーカーコード） 下位 6 ビット
（機種コード）

C + L

意味：先頭から 12 バイト目からのデータ領域に書かれる文字の属性を表す

機能：使用する文字コードと言語コードを各1バイトで表す

50 値：前述のSN1C+Lと同じ

DATA

意味：個別の付加情報データ

機能：可変長データで表す。実データの先頭は常に 1 2 バイト目より始まり、長さ（サイズ）は最小 4 バイト以上、常に 4 バイトの整数倍でなければならない。データの最後から余りがある場合はヌル（0 x 0 0）で埋めること

値：内容により個別に定義される。

【0 0 4 0】以下、トラックデータファイル 1 0 1。～ 1 0 1。について説明する。図 9 は、トラックデータファイル 1 0 1。の構成を説明するための図である。図 9 に示すように、トラックデータファイル 1 0 1。は、1 個のパーツからなり、当該パーツが 5 個のクラスタ CL (0)，CL (1)，CL (2)，CL (3)，CL (4) で構成されている。当該パーツは、クラスタ CL (0) の先頭から開始し、クラスタ CL (4) のサウンドユニット SU (4) で終了している。なお、トラックデータファイル 1 0 1。～ 1 0 1。は、基本的に、図 9 に示す構成をしているが、パーツ数、クラスタ数およびクラスタ内に含まれるサウンドユニット SU の数は、図 9 に示すものには限定されず、独立して決められている。

【0 0 4 1】1 トラックは、1 曲を意味する。1 曲は、1 つの ATRAC3 データファイル（図 6 参照）で構成される。ATRAC3 データファイルは、ATRAC3 により圧縮されたオーディオデータである。メモ리카ード 4 0 に対しては、クラスタと呼ばれる単位で記録される。1 クラスタは、例えば 1 6 K B の容量である。1 クラスタに複数のファイルが混じることがない。フラッシュメモリ 4 2 を消去する時の最小単位が 1 ブロックである。音楽データを記録するのに使用するメモ리카ード 4 0 の場合、ブロックとクラスタは、同意語であり、且つ 1 クラスタ = 1 セクタと定義されている。

【0 0 4 2】1 曲は、基本的に 1 パーツで構成されるが、編集が行われると、複数のパーツから 1 曲が構成されることがある。パーツは、録音開始からその停止までの連続した時間内で記録されたデータの単位を意味し、通常は、1 トラックが 1 パーツで構成される。曲内のパーツのつながりは、各曲の属性ヘッダ内のパーツ情報 PRTINF で管理する。すなわち、パーツサイズは、PRTINF 中のパーツサイズ PRTSIZE という 4 バイトのデータで表す。パーツサイズ PRTSIZE の先頭の 2 バイトがパーツが持つクラスタの総数を示し、続く各 1 バイトが先頭および末尾のクラスタ内の開始サウンドユニット（SU と略記する）の位置、終了 SU の位置を示す。このようなパーツの記述方法を持つことによって、音楽データを編集する際に通常、必要とされる大量の音楽データの移動をなくすることが可能となる。ブロック単位の編集に限定すれば、同様に音楽データの移動を回避できるが、ブロック単位は、SU 単位に比して

編集単位が大きすぎる。

【0 0 4 3】SU は、パーツの最小単位であり、且つ ATRAC3 でオーディオデータを圧縮する時の最小のデータ単位である。4 4. 1 kHz のサンプリング周波数で得られた 1 0 2 4 サンプル分（1 0 2 4 × 1 6 ビット × 2 チャンネル）のオーディオデータを約 1 / 1 0 に圧縮した数百バイトのデータが SU である。1 SU は、時間に換算して約 2 3 m 秒になる。通常は、数千に及ぶ SU によって 1 つのパーツが構成される。1 クラスタが 4 2 個の SU で構成される場合、1 クラスタで約 1 秒の音を表すことができる。1 つのトラックを構成するパーツの数は、付加情報サイズに影響される。パーツ数は、1 ブロックの中からヘッダや曲名、付加情報データ等を除いた数で決まるために、付加情報が全く無い状態が最大数（6 4 5 個）のパーツを使用できる条件となる。

【0 0 4 4】図 1 0 は、1 SU が N バイト（例えば N = 3 8 4 バイト）の場合の ATRAC3 データファイル A 3 D n n n n のデータ配列を示す。図 1 0 には、データファイルの属性ヘッダ（1 ブロック）と、音楽データファイル（1 ブロック）とが示されている。図 1 0 では、この 2 ブロック（1 6 × 2 = 3 2 K バイト）の各スロットの先頭のバイト（0 x 0 0 0 0 ~ 0 x 7 F F 0）が示されている。図 1 1 に分離して示すように、属性ヘッダの先頭から 3 2 バイトがヘッダであり、2 5 6 バイトが曲名領域 NM1（2 5 6 バイト）であり、5 1 2 バイトが曲名領域 NM2（5 1 2 バイト）である。属性ヘッダのヘッダには、下記のデータが書かれる。

【0 0 4 5】BLKID-HD0（4 バイト）

意味：BLOCKID FILE ID

機能：ATRAC3 データファイルの先頭であることを識別するための値

値：固定値 = "HD = 0"（例えば 0 x 4 8 4 4 2 D 3 0）

MCODE（2 バイト）

意味：MAKER CODE

機能：記録した機器の、メーカー、モデルを識別するコード

値：上位 1 0 ビット（メーカーコード） 下位 6 ビット（機種コード）

BLOCK SERIAL（4 バイト）

意味：トラック毎に付けられた連続番号

機能：ブロックの先頭は 0 から始まり次のブロックは + 1 づつインクリメント編集されても値を変化させない

値：0 より始まり 0 x F F F F F F F F まで。

【0 0 4 6】N1C+L（2 バイト）

意味：トラック（曲名）データ（NM1）の属性を表す

機能：NM1 に使用される文字コードと言語コードを各 1 バイトで表す

値：SN1C+L と同一

N2C+L（2 バイト）

意味：トラック（曲名）データ（NM2）の属性を表す
機能：NM2に使用される文字コードと言語コードを各1バイトで表す

値：SN1C+Lと同一

INFSIZE（2バイト）

意味：トラックに関する付加情報の全てを合計したサイズを表す

機能：データサイズを16バイト単位の大きさを記述、無い場合は必ずオールゼロとすること

値：サイズは0x0000から0x3C6（966）

TPRT（2バイト）

意味：トータルパーツ数

機能：トラックを構成するパーツ数を表す。通常は1

値：1から0x285（645dec）

T-SU（4バイト）

意味：トータルSU数

機能：1トラック中の実際の総SU数を表す。曲の演奏時間に相当する

値：0x01から0x001FFFFFFF

INX（2バイト）（Option）

意味：INDEXの相対場所

機能：曲のさびの部分（特徴的な部分）の先頭を示すポインタ。曲の先頭からの位置をSUの個数を1/4した数で指定する。これは、通常のSUの4倍の長さの時間（約93m秒）に相当する

値：0から0xFFFF（最大、約6084秒）

XT（2バイト）（Option）

意味：INDEXの再生時間

機能：INX-nnnで指定された先頭から再生すべき時間のSUの個数を1/4した数で指定する。これは、通常のSUの4倍の長さの時間（約93m秒）に相当する

値：0x0000：無設定 0x01から0xFFFFE（最大6084秒）

0xFFFFF：曲の終わりまで。

【0047】次に曲名領域NM1およびNM2について説明する。

【0048】NM1

意味：曲名を表す文字列

機能：1バイトの文字コードで表した可変長の曲名（最大で256）

名前データの終了は、必ず終端コード（0x00）を書き込むこと

サイズはこの終端コードから計算すること、データの無い場合は少なくとも先頭（0x0020）からヌル（0x00）を1バイト以上記録すること

値：各種文字コード

NM2

意味：曲名を表す文字列

機能：2バイトの文字コードで表した可変長の名前データ（最大で512）

名前データの終了は、必ず終端コード（0x00）を書き込むこと

サイズはこの終端コードから計算すること、データの無い場合は少なくとも先頭（0x0120）からヌル（0x00）を2バイト以上記録すること

値：各種文字コード。

【0049】属性ヘッダの固定位置（0x320）から始まる、80バイトのデータをトラック情報領域TRKINFと呼び、主としてセキュリティ関係、コピー制御関係の情報を一括して管理する。図12にTRKINFの部分を示す。TRKINF内のデータについて、配置順序に従って以下に説明する。

【0050】CONTENTS KEY（8バイト）

意味：曲毎に用意された値で、メモ리카ードのセキュリティブロックで保護されてから保存される

機能：曲を再生する時、まず必要となる最初の鍵となる。MAC計算時に使用される

値：0から0xFFFFFFFFFFFFFFFFまでMAC（8バイト）

20 意味：著作権情報改ざんチェック値

機能：コンテンツ累積番号を含む複数のTRKINFの内容と隠しシーケンス番号から作成される値

隠しシーケンス番号とは、メモ리카ードの隠し領域に記録されているシーケンス番号のことである。著作権対応でないレコーダは、隠し領域を読むことができない。また、著作権対応の専用のレコーダ、またはメモ리카ードを読むことを可能とするアプリケーションを搭載したパーソナルコンピュータは、隠し領域をアクセスすることができる。

30 【0051】A（1バイト）

意味：パーツの属性

機能：パーツ内の圧縮モード等の情報を示す

値：図13を参照して以下に説明する

ただし、N=0, 1のモノラルは、bit7が1でサブ信号を0、メイン信号（L+R）のみの特別なJoinモードをモノラルとして規定する。bit2, 1の情報は通常の再生機は無視しても構わない。

【0052】Aのビット0は、エンファシスのオン／オフの情報を形成し、ビット1は、再生SKIPか、通常再生かの情報を形成し、ビット2は、データ区分、例えばオーディオデータか、FAX等の他のデータかの情報を形成する。ビット3は、未定義である。ビット4、5、6を組み合わせてことによって、図示のように、ATRAC3のモード情報が規定される。すなわち、Nは、この3ビットで表されるモードの値であり、モノ（N=0, 1）、LP（N=2）、SP（N=4）、EX（N=5）、HQ（N=7）の5種類のモードについて、記録時間（64MBのメモ리카ードの場合）、データ転送レート、1ブロック内のSU数がそれぞれ示されている。1SUのバイト数は、（モノ：136バイト、

LP: 192バイト、SP: 304バイト、EX: 384バイト、HQ: 512バイト)である。さらに、ビット7によって、ATRC3のモード(0: Dual 1: Joint)が示される。

【0053】一例として、64MBのメモリカードを使用し、SPモードの場合について説明する。64MBのメモリカードには、3968ブロックがある。SPモードでは、1SUが304バイトであるので、1ブロックに53SUが存在する。1SUは、(1024/44100)秒に相当する。従って、1ブロックは、

(1024/44100) × 53 × (3968 - 16) = 4863秒 = 81分

転送レートは、

(44100/1024) × 304 × 8 = 104737 bps

となる。

【0054】LT (1バイト)

意味: 再生制限フラグ(ビット7およびビット6)とセキュリティバージョン

(ビット5~ビット0)

機能: このトラックに関して制限事項があることを表す

値: ビット7: 0 = 制限なし 1 = 制限有り

ビット6: 0 = 期限内 1 = 期限切れ

ビット5~ビット0: セキュリティバージョン0 (0以外であれば再生禁止とする)

FNo (2バイト)

意味: ファイル番号

機能: 最初に記録された時のトラック番号、且つこの値は、メモリカード内の隠し領域に記録されたMAC計算用の値の位置を特定する

値: 1から0x190 (400)

MG (D) SERIAL-nnn (16バイト)

意味: 記録機器のセキュリティブロック(セキュリティIC20)のシリアル番号

機能: 記録機器ごとに全て異なる固有の値

値: 0から0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

CONNUM (4バイト)

意味: コンテンツ累積番号

機能: 曲毎に累積されていく固有の値で記録機器のセキュリティブロックによって管理される。2の32乗、42億曲分用意されており、記録した曲の識別に使用する

値: 0から0xFFFFFFFF

【0055】

YMDhms-S (4バイト) (Option)

意味: 再生制限付きのトラックの再生開始日時

機能: EMDで指定する再生開始を許可する日時

値: 上述した日時の表記と同じ

YMDhms-E (4バイト) (Option)

意味: 再生制限付きのトラックの再生終了日時

機能: EMDで指定する再生許可を終了する日時

値: 上述した日時の表記と同じ

MT (1バイト) (Option)

意味: 再生許可回数の最大値

機能: EMDで指定される最大の再生回数

値: 1から0xFF 未使用の時は、0x00

LTのビット7の値が0の場合はMTの値は00とすること

CT (1バイト) (Option)

意味: 再生回数

10 機能: 再生許可された回数の内で、実際に再生できる回数。再生の度にデクリメントする

値: 0x00~0xFF 未使用の時は、0x00であるLTのビット7が1でCTの値が00の場合は再生を禁止すること。

【0056】CC (1バイト)

意味: COPY CONTROL

機能: コピー制御

値: 図14に示すように、ビット6および7によってコピー制御情報を表し、ビット4および5によって高速デジタルコピーに関するコピー制御情報を表し、ビット2および3によってセキュリティブロック認証レベルを表す。ビット0および1は、未定義

20 CCの例: (ビット7, 6) 11: 無制限のコピーを許可、01: コピー禁止、00: 1回のコピーを許可

(ビット3, 2) 00: アナログないしデジタルインからの録音、MG認証レベルは0とする

CDからのデジタル録音では(ビット7, 6)は00、(ビット3, 2)は00となる

CN (1バイト) (Option)

30 意味: 高速デジタルコピーHSCMS (High speed Serial Copy Management System)におけるコピー許可回数

機能: コピー1回か、コピーフリーかの区別を拡張し、回数で指定する。コピー第1世代の場合にのみ有効であり、コピーごとに減算する

値: 00: コピー禁止、01から0xFE: 回数、0xFF: 回数無制限。

【0057】上述したトラック情報領域TRKINFに続いて、0x0370から始まる24バイトのデータをパーツ管理用のパーツ情報領域PRTINFと呼び、1つのトラックを複数のパーツで構成する場合に、時間軸の順番にPRTINFを並べていく。図15にPRTINFの部分を示す。PRTINF内のデータについて、配置順序に従って以下に説明する。

【0058】PRTSIZE (4バイト)

意味: パーツサイズ

機能: パーツの大きさを表す。クラスタ: 2バイト(最上位)、開始SU: 1バイト(上位)、終了SU: 1バイト(最下位)

値: クラスタ: 1から0x1F40 (8000)、開始SU: 0から0xA0 (160)、終了SU: 0から0

x A 0 (1 6 0) (但し、S U の数え方は、0, 1, 2, と 0 から開始する)

P R T K E Y (8 バイト)

意味：パーツを暗号化するための値

機能：初期値 = 0、編集時は編集の規則に従うこと

値：0 から 0 x F F F F F F F F F F F F F F F F

C O N N U M 0 (4 バイト)

意味：最初に作られたコンテンツ累積番号キー

機能：コンテンツをユニークにするための I D の役割

値：コンテンツ累積番号初期値キーと同じ値とされる。 10

【0059】A T R A C 3 データファイルの属性ヘッダ中には、図 10 に示すように、付加情報 I N F が含まれる。この付加情報は、開始位置が固定化されていない点を除いて、再生管理ファイル中の付加情報 I N F - S (図 7 および図 8 B 参照) と同一である。1 つまたは複数のパーツの最後のバイト部分 (4 バイト単位) の次を開始位置として付加情報 I N F のデータが開始する。

【0060】I N F

意味：トラックに関する付加情報データ

機能：ヘッダを伴った可変長の付加情報データ。複数の異なる付加情報が並べられることがある。それぞれに I D とデータサイズが付加されている。個々のヘッダを含む付加情報データは、最小 1 6 バイト以上で 4 バイトの整数倍の単位 20

値：再生管理ファイル中の付加情報 I N F - S と同じである。

【0061】上述した属性ヘッダに対して、A T R A C 3 データファイルの各ブロックのデータが続く。図 1 6 に示すように、ブロック毎にヘッダが付加される。各ブロックのデータについて以下に説明する。

【0062】B L K I D - A 3 D (4 バイト)

意味：B L O C K I D F I L E I D

機能：A T R A C 3 データの先頭であることを識別するための値

値：固定値 = " A 3 D " (例えば 0 x 4 1 3 3 4 4 2 0)

M C o d e (2 バイト)

意味：M A K E R C O D E

機能：記録した機器の、メーカー、モデルを識別するコード

値：上位 1 0 ビット (メーカーコード) 下位 6 ビット (機種コード)

C O N N U M 0 (4 バイト)

意味：最初に作られたコンテンツ累積番号

機能：コンテンツをユニークにするための I D の役割、編集されても値は変化させない

値：コンテンツ累積番号初期値キーと同じ値とされる

B L O C K S E R I A L (4 バイト)

意味：トラック毎に付けられた連続番号

機能：ブロックの先頭は 0 から始まり次のブロックは + 50

1 づつインクリメント編集されても値を変化させない

値：0 より始まり 0 x F F F F F F F F F F F F F F F F

B L O C K - S E E D (8 バイト)

意味：1 ブロックを暗号化するための 1 つの鍵

機能：ブロックの先頭は、記録機器のセキュリティブロックで乱数を生成、続くブロックは、+ 1 インクリメントされた値、この値が失われると、1 ブロックに相当する約 1 秒間、音が出せないために、ヘッダとブロック末尾に同じものが二重に書かれる。編集されても値を変化させない

値：初期は 8 バイトの乱数

I N I T I A L I Z A T I O N V E C T O R (8 バイト)

意味：ブロック毎に A T R A C 3 データを暗号化、復号化する時に必要な初期値

機能：ブロックの先頭は 0 から始まり、次のブロックは最後の S U の最後の暗号化された 8 バイトの値。デバインドされたブロックの途中からの場合は開始 S U の直前の最後の 8 バイトを用いる。編集されても値を変化させない 20

値：0 から 0 x F F F F F F F F F F F F F F F F

S U - n n n

意味：サウンドユニットのデータ

機能：1 0 2 4 サンプルから圧縮されたデータ、圧縮モードにより出力されるバイト数が異なる。編集されても値を変化させない (一例として、S P モードの時では、N = 3 8 4 バイト)

値：A T R A C 3 のデータ値。

【0063】図 10 では、N = 3 8 4 であるので、1 ブロックに 4 2 S U が書かれる。また、1 ブロックの先頭の 2 つのスロット (4 バイト) がヘッダとされ、最後の 1 スロット (2 バイト) に B L K I D - A 3 D、M C o d e、C O N N U M 0、B L O C K S E R I A L が二重に書かれる。従って、1 ブロックの余りの領域 M バイトは、(1 6, 3 8 4 - 3 8 4 x 4 2 - 1 6 x 3 = 2 0 8 (バイト)) となる。この中に上述したように、8 バイトの B L O C K S E E D が二重に記録される。 30

【0064】また、サウンドユニット S U (0) ~ (1 0 1) は、図 2 に示す暗号化 / 復号ユニット 6 4 において C B C (C i p h e r B l o c k C h a i n n i n g) モードで 6 4 ビット (8 バイト) の暗号化ブロックを単位として暗号化して生成された 8 バイトの暗号文 C_i によって構成される。本実施形態では、サウンドユニット S U のバイト数 (例えば 1 6 0 バイト) を、暗号化の単位である暗号化ブロックのバイト数 (例えば 8 バイト) の整数倍にしている。すなわち、1 サウンドユニット S U は例えば 2 0 個の暗号文 C_i からなる。このとき、個々の暗号文 C_i は一のサウンドユニット S U 内に位置し、一の暗号文 C_i が複数のサウンドユニット S U に跨って位置することはない。 40 50

【0065】ここで、フラッシュメモリ34に記憶されているオーディオデータは、後述するように例えば、ATRAC3方式で圧縮されており、当該圧縮の単位がサウンドユニットSUである。従って、携帯用記憶装置3から携帯用プレーヤ4にオーディオデータを読み出す場合には、読み出しの最小単位は当該サウンドユニットSUとなる。

【0066】このようにすることで、フラッシュメモリ34に記憶されている暗号化されたオーディオデータにアクセスする際に、暗号化ブロックの区切りを意識する必要がなくなり、当該アクセスに伴う処理負担を軽減できる。なお、各クラスタ内に含まれるサウンドユニットSUの数は、1個以上102個以下の範囲で任意である。また、オーディオデータの圧縮方式は、ATRAC3などのATRAC方式以外のCODEC方式でもよい。

【0067】ブロックシードデータBSは、各ブロック毎に例えば乱数を発生して生成されたデータであり、後述するように、携帯用プレーヤ4内でブロック毎にブロック鍵データBKを生成する際に用いられる。当該ブロックシードデータBSは、エラー対策としてブロック内の2箇所に格納されている。なお、各クラスタに含まれるサウンドユニットは、暗号化された順でフラッシュメモリ34の連続したアドレスに記憶される。また、各サウンドユニット内の暗号化ブロックは、暗号化された順にフラッシュメモリ34の連続したアドレスに記憶される。

【0068】〔フラッシュメモリ管理モジュール35〕フラッシュメモリ管理モジュール35は、フラッシュメモリ34へのデータの書き込み、フラッシュメモリ34からのデータの読み出しなどの制御を行う。

【0069】携帯用プレーヤ4図2に示すように、携帯用プレーヤ4は、例えば、主制御モジュール41、通信

$$IK_j = f(MK_j, ID_i)$$

但し、iは、 $0 \leq j \leq 31$ の整数。

【0074】また、記憶ユニット61における認証鍵データIK。 \sim IK₃₁の記憶アドレスは、例えば5ビットで表現され、それぞれ記憶ユニット51におけるマスター鍵データMK。 \sim MK₃₁と同じ記憶アドレスが割り当てられている。

【0075】鍵生成／鍵演算ユニット62は、例えば、ISO/IEC9797のMAC演算方式を用いた演算などの種々の演算を行って鍵データを生成する。このとき、"Block cipher Algorithm"としてFIPS PUB 46-2に規定されるDESが用いられる。

【0076】相互認証ユニット63は、例えば、コンピュータ2から入力したオーディオデータを携帯用記憶装置3に出力する動作を行うのに先立って、携帯用記憶装置3との間で相互認証処理を行う。また、相互認証ユニット63は、携帯用記憶装置3からオーディオデータを

インターフェイス42、制御モジュール43、編集モジュール44、圧縮／伸長モジュール45、スピーカ46、D/A変換器47およびA/D変換器48を有する。

【0070】〔主制御モジュール41〕主制御モジュール41は、携帯用プレーヤ4の処理を統括的に制御する。

【0071】〔制御モジュール43〕図2に示すように、制御モジュール43は、例えば、乱数発生ユニット60、記憶ユニット61、鍵生成／鍵演算ユニット62、相互認証ユニット63、暗号化／復号ユニット64および制御ユニット65を有する。制御モジュール43は、制御モジュール33と同様に、シングルチップの暗号処理専用の集積回路であり、多層構造を有し、内部のメモリセルはアルミニウム層などのダミー層に挟まれている。また、制御モジュール43は、動作電圧または動作周波数の幅が狭く、外部から不正にデータを読み出せないように耐タンパー性を有している。乱数発生ユニット60は、乱数発生指示を受けると、64ビット（8バイト）の乱数を発生する。記憶ユニット61は、認証処理に必要な種々のデータを記憶している。

【0072】図17は、記憶ユニット61に記憶されているデータを説明するための図である。図17に示すように、記憶ユニット61は、マスター鍵データMK。 \sim MK₃₁および装置識別データID_iを記憶している。ここで、マスター鍵データMK。 \sim MK₃₁と、認証鍵データIK。 \sim IK₃₁の間には、前述した携帯用記憶装置3の装置識別データID_iを用いて、下記式（1）に示す関係がある。なお、下記式において、f(a, b)は、例えば、引数a, bから値を導出する関数である。

【0073】

【数1】

・・・（1）

入力する動作を行うのに先立って、携帯用記憶装置3との間で相互認証処理を行う。また、相互認証ユニット63は、相互認証処理において、前述したMAC演算を行う。当該相互認証処理では、記憶ユニット61に記憶されているデータが用いられる。なお、相互認証ユニット63は、必要に応じて、例えば、コンピュータ2あるいはネットワーク5上のコンピュータとの間でオーディオデータの入出力を行う動作に先立って、コンピュータ2あるいはネットワーク5上のコンピュータとの間で相互認証処理を行う。

【0077】暗号化／復号ユニット64は、前述したように、FIPS PUB 81に規定されたECBモードおよびCBCモードを選択的に用いてブロック暗号化を行う。ここで、暗号化／復号ユニット64は、CBCモードにおいて、56ビットの鍵データkを用いて、コンピュータ2あるいはCDプレーヤ7から入力したオー

ディオデータ（平文）を、64ビットからなる暗号化ブロックを単位として下記式（2）に基づいて暗号化して暗号化されたオーディオデータ（暗号文）を生成する。下記式（2）から分かるように、CBCモードでは、一つ前の暗号文と次の平文との排他的論理和を暗号化する

$$C_i = E_k (P_i \text{ XOR } C_{i-1})$$

i : 1以上の整数

P_i : 平文（64ビット）

C_i : 暗号文（64ビット）

XOR : 排他的論理和

E_k : 56ビットの鍵データ k を用いたDES方式の暗号処理

上記式（2）の演算は、図18で表現される。なお、図18において、「IV」は、ブロック暗号化初期値（64ビット）であり、図2に示す携帯用記憶装置3のフラッシュメモリ34において、図8に示すようにクラスタCL内のサウンドユニットSU（0）の直前に記憶される。

【0079】なお、コンピュータ2あるいはCDプレーヤ7から入力したオーディオデータ（平文）は、ATRAC（Adaptive Transform Audio Coder）方式を改良したATRAC3方式で圧縮されている。なお、ATRACは、MD（Mini Disk：商標）のための符号化圧縮方式

$$P_i = C_{i-1} \text{ XOR } D_k (C_i)$$

i : 1以上の整数

P_i : 平文（64ビット）

C_i : 暗号文（64ビット）

XOR : 排他的論理和

D_k : 56ビットの鍵データ k を用いたDES方式の復号処理

上記式（3）の演算は、図19で表現される。なお、図19において、「IV」は、ブロック暗号化初期値（64ビット）であり、図2に示す携帯用記憶装置3のフラッシュメモリ34において図8に示すようにクラスタCL内のサウンドユニットSU（0）の直前に記憶されたものが用いられる。

【0082】制御ユニット65は、乱数発生ユニット60、記憶ユニット61、鍵生成／鍵演算ユニット62、相互認証ユニット63および暗号化／復号ユニット64の処理を統括的に制御する。

【0083】〔編集モジュール44〕編集モジュール44は、例えば、図4に示すように携帯用記憶装置3のフラッシュメモリ34内に記憶されたトラックデータファイル101。～101。を、ユーザからの操作指示に基づいて編集して新たなトラックデータファイルを生成する。当該編集には、1個のトラックデータファイルを分割して2個のトラックデータファイルを生成する分割編集処理と、2個のトラックデータファイルを結合して1個のトラックデータファイルを生成する結合編集処理とがある。なお、当該編集にあたって、再生管理ファイル

ため、同一の平文が入力されても異なる暗号文が出力され、解読が困難であるという利点がある。

【0078】

【数2】

・・・（2）

あり、例えば、288kbit/sで44.1kHzサンプルのステレオ信号が、帯域分割とMDCT（Modified Discrete Cosine Transform）とを併用して符号化されている。すなわち、まず、帯域分割フィルタで1/4、1/4、1/2の3つの帯域に分割され、それぞれの帯域の信号がダウンサンプルされ、時間領域の信号としてMDCTで周波数領域に変換され、当該MDCTの係数が適応ビット配分を行ってスカラー量子化されている。

【0080】暗号化／復号ユニット64は、FIPS81のモードのうち、前述したECBモードおよびCBCモードの復号を選択的に行う。ここで、暗号化／復号ユニット64は、CBCモードにおいて、56ビットの鍵データ k を用いて、暗号文を、64ビットからなる暗号化ブロックを単位として下記式（3）に基づいて復号して平文を生成する。

【0081】

【数3】

・・・（3）

100およびトラックデータファイル101。～101。が書き換えられる。編集モジュール44における編集処理については後に詳細に説明する。

【0084】〔圧縮／伸長モジュール45〕圧縮／伸長モジュール45は、例えば、携帯用記憶装置3から入力した暗号化されたオーディオデータを復号した後に再生する際に、ATRAC3方式で圧縮されているオーディオデータを伸長し、当該伸長したオーディオデータをD/A変換器47に出力する。また、例えば、CDプレーヤ7あるいはコンピュータ2から入力したオーディオデータを、携帯用記憶装置3に記憶する際に、当該オーディオデータをATRAC3方式で圧縮する。

【0085】〔D/A変換器47〕D/A変換器47は、圧縮／伸長モジュール45から入力したデジタル形式のオーディオデータをアナログ形式のオーディオデータに変換してスピーカ46に出力する。

【0086】〔スピーカ46〕スピーカ46は、D/A変換器47から入力したオーディオデータに応じた音響を出力する。

【0087】〔A/D変換器48〕A/D変換器48は、例えば、CDプレーヤ7から入力したアナログ形式のオーディオデータをデジタル形式に変換して圧縮／伸長モジュール45に出力する。

【0088】以下、図1に示すオーディオシステム1の動作について説明する。

【0089】携帯用記憶装置3への書き込み動作図20

は、携帯用プレーヤ4から携帯用記憶装置3への書き込み動作を説明するためのフローチャートである。

【0090】ステップS1：携帯用プレーヤ4から携帯用記憶装置3に、書き込み要求信号が出力される。

【0091】ステップS2：携帯用記憶装置3と携帯用プレーヤ4との間で、相互認証処理を行う際に用いる認証鍵データ IK_j の選択処理が行われる。当該処理については後述する。

【0092】ステップS3：携帯用記憶装置3と携帯用プレーヤ4との間で相互認証処理が行われる。当該処理については後述する。

【0093】ステップS4：ステップS3の相互認証処理によって携帯用記憶装置3および携帯用プレーヤ4の双方が相手を正当であると認めた場合には、ステップS5の処理が行われ、そうでない場合には処理が終了する。

【0094】ステップS5：携帯用記憶装置3および携帯用プレーヤ4において、セッション鍵データ Se_k が生成される。当該処理については後述する。

【0095】ステップS6：携帯用プレーヤ4から携帯用記憶装置3に、通信インターフェイス32、42を介して、暗号化したオーディオデータを出力して書き込む。当該処理については後述する。

【0096】このように、オーディオシステム1によれば、携帯用記憶装置3と携帯用プレーヤ4との間で相互認証が行われ、双方が相手を正当であると認めた場合にのみ、携帯用プレーヤ4から携帯用記憶装置3に、暗号化されたオーディオデータが書き込まれる。そのため、

$$IK_j = f(MK_j, ID.)$$

これにより、携帯用記憶装置3と携帯用プレーヤ4とが、上記式(4)に示す関係を持つ認証鍵データ $IK_0 \sim IK_{31}$ およびマスター鍵データ $MK_0 \sim MK_{31}$ を有している場合には、図21に示す処理によって同じ認証鍵データ IK_j が選択される。当該選択された認証鍵データ IK_j は、後述する相互認証処理を行う際に、秘密鍵として用いられる。また、このとき、32個の認証鍵データ IK_j のうち選択される認証鍵データは、図21に示す処理を行う毎に乱数 R_j に応じてランダムに決定される。そのため、不正な認証が成功する確率を、一の認証鍵データを固定して用いる場合の $1/32$ 倍にすることができ、不正な認証が行われることを高い確率で回避できる。

【0102】なお、上述した実施形態では、乱数を用いて8個の認証鍵データ IK_j のうちの認証鍵データを選択する場合を例示したが、携帯用記憶装置3および携帯用プレーヤ4の外部から入力した鍵指定信号に基づいて選択する認証鍵データを決定してもよい。

【0103】〔携帯用記憶装置3と携帯用プレーヤ4との間の相互認証処理(図20に示すステップS3)〕図22は、携帯用記憶装置3と携帯用プレーヤ4との間の

著作権侵害を招くようなオーディオデータの不正な複製が容易に行われることを回避できる。

【0097】〔認証鍵データ IK_j の選択処理(図20に示すステップS2)〕図21は、認証鍵データ IK_j の選択処理を説明するための図である。図21に示すように、図2に示す携帯用プレーヤ4の乱数発生ユニット60によって64ビットの乱数 R_j が生成される。当該乱数 R_j は、携帯用プレーヤ4から携帯用記憶装置3に出力される。そして、携帯用記憶装置3の相互認証ユニット53によって、64ビットの乱数 R_j の下位5ビットを用いて、記憶ユニット51に記憶されている認証鍵データ $IK_0 \sim IK_{31}$ のうちの認証鍵データ IK_j (j は $0 \leq j \leq 31$ を満たす整数)が特定される。

【0098】また、携帯用記憶装置3の記憶ユニット51から読み出された装置識別データ ID_j が、携帯用記憶装置3から携帯用プレーヤ4に出力される。

【0099】そして、携帯用プレーヤ4の相互認証ユニット63によって、乱数 R_j の下位5ビットを用いて、マスター鍵データ $MK_0 \sim MK_{31}$ のうちのマスター鍵データ MK_j が特定される。

【0100】そして、鍵生成/鍵演算ユニット62において、前記特定されたマスター鍵データ MK_j と、携帯用記憶装置3から入力した装置識別データ ID_j とを用いて、下記式(4)に基づいて、認証鍵データ IK_j を生成する。下記式(4)において、 $f(a, b)$ は、例えば、引数 a, b から値を導出する任意の関数である。

【0101】

【数4】

$$\dots (4)$$

相互認証処理を説明するための図である。なお、当該相互認証処理を開始するときには、前述した図21に示す認証鍵データ IK_j の選択処理が終了しており、携帯用プレーヤ4の相互認証ユニット53と携帯用記憶装置3の相互認証ユニット63は、選択した認証鍵データ IK_j 、携帯用記憶装置3の装置識別データ ID_j を有している。

【0104】ステップS10：携帯用記憶装置3の乱数発生ユニット50において、64ビットの乱数 R_s を生成し、これを携帯用プレーヤ4に出力する。

【0105】ステップS11：携帯用プレーヤ4の乱数発生ユニット60において、64ビットの乱数 R_d および S_d を生成する。

【0106】ステップS12：携帯用プレーヤ4の相互認証ユニット63において、図20に示すステップS2で得た認証鍵データ IK_j および「 $R_d \parallel R_s \parallel ID_j$ 」を用いて、下記式(5)に基づいてMAC演算を行い、 MAC_j を求める。

【0107】ここで、 $A \parallel B$ は、 A と B の連結(n ビットの A の後ろに m ビットの B を結合して($n+m$)ビットとしたもの)を示す。

【0108】

$$MAC_A = MAC(IK_j, R_d \parallel R_{s,j} \parallel ID_{s,j}) \quad \dots (5)$$

ステップS13：携帯用プレーヤ4は、「 $R_d \parallel S_d \parallel MAC_A \parallel j$ 」を携帯用記憶装置3に出力する。

【0109】ステップS14：携帯用記憶装置3の相互認証ユニット53において、図20に示すステップS2で得た認証鍵データ IK_j および「 $R_d \parallel R_{s,j} \parallel I$

$$MAC_s = MAC(IK_j, R_d \parallel R_{s,j} \parallel ID_{s,j}) \quad \dots (6)$$

ステップS15：携帯用記憶装置3の相互認証ユニット53において、ステップS14で求めた MAC_s とステップS13で入力した MAC_A とを比較し、一致していれば、携帯用プレーヤ4が適切な認証鍵データ IK_j を有していることが分かるため、携帯用記憶装置3は携帯用プレーヤ4が正当な相手であると認証する。

【0111】ステップS16：携帯用記憶装置3の相互

$$MAC_c = MAC(IK_j, R_{s,j} \parallel R_d) \quad \dots (7)$$

ステップS17：携帯用記憶装置3の乱数発生ユニット50において、64ビットの乱数 $S_{s,j}$ を生成する。

【0113】ステップ18：携帯用記憶装置3から携帯用プレーヤ4に、「 $S_{s,j} \parallel MAC_c$ 」を出力する。

【0114】ステップS19：携帯用プレーヤ4の相互

$$MAC_d = MAC(IK_j, R_{s,j} \parallel R_d) \quad \dots (8)$$

ステップS20：携帯用プレーヤ4の相互認証ユニット63において、ステップS19で求めた MAC_d とステップS18で入力した MAC_c とを比較し、一致していれば、携帯用記憶装置3が適切な認証鍵データ IK_j を有していることが分かるため、携帯用プレーヤ4は携帯用記憶装置3が正当な相手であると認証する。以上の処理によって、携帯用記憶装置3と携帯用プレーヤ4との間の相互認証が行われる。

【0116】〔セッション鍵データ Se_k の生成処理（図20に示すステップS5）〕図23は、セッション鍵データ Se_k の生成処理を説明するための図である。なお、当該セッション鍵データ Se_k の生成処理を開始

$$セッション鍵データ $Se_k = MAC(IK_j, S_d \parallel S_{s,j}) \quad \dots (9)$$$

ステップS31：携帯用記憶装置3の相互認証ユニット53は、選択した認証鍵データ IK_j および「 $S_d \parallel S_{s,j}$ 」を用いて、下記式(10)に基づいてMAC演算を行い、セッション鍵データ Se_k を生成する。当該セッション鍵データ Se_k は、正当な相手同士であれば、携

$$セッション鍵データ $Se_k = MAC(IK_j, S_d \parallel S_{s,j}) \quad \dots (10)$$$

〔携帯用記憶装置3へのオーディオデータの書き込み処理（図20に示すステップS6）〕図24は、携帯用プレーヤ4から携帯用記憶装置3へのオーディオデータの書き込み処理を説明するための図である。なお、当該書き込み処理を開始するときには、前述した図23に示すセッション鍵データ Se_k の生成処理は終了しており、携帯用記憶装置3および携帯用プレーヤ4は同じセッション鍵データ Se_k を有している。

【0120】ステップS40：携帯用プレーヤ4は、乱

【数5】

$D_{s,j}$ 」を用いて、下記式(6)に基づいてMAC演算を行い、 MAC_s を求める。

【0110】

【数6】

認証ユニット53において、図20に示すステップS2で得た認証鍵データ IK_j および「 $R_{s,j} \parallel R_d$ 」を用いて、下記式(7)に基づいてMAC演算を行い、 MAC_c を求める。

【0112】

【数7】

認証ユニット63において下記式(8)に基づいてMAC演算を行い、 MAC_d を求める。

【0115】

【数8】

するときには、前述した図21に示す認証鍵データ IK_j の選択処理および図22に示す相互認証処理が終了しており、携帯用記憶装置3および携帯用プレーヤ4の双方は、選択した認証鍵データ IK_j および乱数 S_d 、 $S_{s,j}$ を有している。

【0117】ステップS30：携帯用プレーヤ4の相互認証ユニット63は、選択した認証鍵データ IK_j および「 $S_d \parallel S_{s,j}$ 」を用いて、下記式(9)に基づいてMAC演算を行い、セッション鍵データ Se_k を生成する。

【0118】

【数9】

携帯用プレーヤ4で生成したセッション鍵データ Se_k と同じになる。

【0119】

【数10】

乱数発生ユニット60にトラックデータファイル毎に乱数を発生させ、当該乱数に応じたコンテンツ鍵データ CK を生成する。

【0121】ステップS41：携帯用プレーヤ4は、暗号化／復号ユニット64において、ステップS40で生成したコンテンツ鍵データ CK を、セッション鍵データ Se_k を用いて暗号化する。

【0122】ステップ42：携帯用プレーヤ4は、ステップS41で暗号化したコンテンツ鍵データ CK を携帯

用記憶装置 3 に出力する。

【0123】ステップ S 43：携帯用記憶装置 3 は、ステップ S 42 で入力した暗号化されたコンテンツ鍵データ CK を、暗号化／復号ユニット 54 において復号する。

【0124】ステップ S 44：携帯用記憶装置 3 は、暗号化／復号ユニット 54 において、ステップ S 43 で復号したコンテンツ鍵データ CK を、記憶ユニット 51 から読み出した記憶用鍵データ SK_m を用いて暗号化する。

【0125】ステップ S 45：携帯用記憶装置 3 は、当該暗号化されたコンテンツ鍵データ CK を携帯用プレーヤ 4 に出力する。

【0126】ステップ S 46：携帯用プレーヤ 4 は、当該暗号化されたコンテンツ鍵データ CK を、トラックデータファイル 100n 内の TRK INF 内に設定する。

【0127】ステップ S 47：携帯用プレーヤ 4 は、乱

$$TMK = PK \text{ XOR } CK$$

ステップ S 49：携帯用プレーヤ 4 は、乱数発生ユニット 60 にブロック毎に乱数を発生させ、当該乱数に応じたブロックシードデータ BS を生成する。また、携帯用プレーヤ 4 は、当該生成したブロックシードデータ BS を、当該ブロック内の図 10 に示す対応する位置に設定する。

【0130】ステップ S 50：携帯用プレーヤ 4 は、例

$$BK = MAC(TMK, BS)$$

なお、MAC 演算の他に、例えば、SHA-1 (Secure Hash Algorithm)、RIPMD-160 などの一方向性ハッシュ関数 (one-way hash function) の入力に秘密鍵を用いた演算を行ってブロック鍵データ BK を生成してもよい。

【0132】ここで、一方向性関数 f とは、 x より $y = f(x)$ を計算することは容易であるが、逆に y より x を求めることが難しい関数をいう。一方向性ハッシュ関数については、例えば、“Handbook of Applied Cryptography, CRC Press”などに詳しく記述されている。

【0133】ステップ S 51：携帯用プレーヤ 4 は、コンピュータ 2 あるいは携帯用プレーヤ 4 から入力したオーディオデータを、圧縮／伸長モジュール 45 において、ATRAC3 方式で圧縮する。そして、暗号化／復号ユニット 64 において、ステップ S 50 で生成したブロック鍵データ BK を用いて、前記圧縮したオーディオデータを CBC モードで暗号化する。

【0134】ステップ S 52：携帯用プレーヤ 4 は、ステップ S 51 で暗号化したオーディオデータに属性ヘッダを付加して、通信インターフェイス 32、42 を介して、携帯用記憶装置 3 に出力する。

【0135】ステップ S 53：携帯用記憶装置 3 は、ステップ S 52 で入力した暗号化されたオーディオデータと属性ヘッダを、フラッシュメモリ 34 にそのまま書き

数発生ユニット 60 にパーツ毎に乱数を発生させ、当該乱数に応じたパーツ鍵データ PK を生成する。また、携帯用プレーヤ 4 は、当該生成したパーツ鍵データ PK を、トラックデータファイル 101n の管理データ PR TINF 内に設定する。

【0128】ステップ S 48：携帯用プレーヤ 4 は、例えば、パーツ毎に、鍵生成／演算ユニット 62 において、下記式 (11) に示すように、ステップ S 47 で生成したパーツ鍵データ PK とコンテンツ鍵データ CK との排他的論理和を演算し、当該演算結果をテンポラリ鍵データ TMK とする。なお、テンポラリ鍵データ TMK の生成は、排他的論理和を用いるものには限定されず、例えば、パーツ鍵データ PK とコンテンツ鍵データ CK とを加算する加算演算やその他の関数演算を用いるようにしてもよい。

【0129】

【数 11】

・・・ (11)

例えば、鍵生成／鍵演算ユニット 62 において、下記式 (12) に示すように、ステップ S 46 で生成したテンポラリ鍵データ TMK と、ステップ S 47 で生成したブロックシードデータ BS とを用いて MAC 演算を行い、ブロック毎にブロック鍵データ BK を生成する。

【0131】

【数 12】

・・・ (12)

込む。以上の処理によって、携帯用プレーヤ 4 から携帯用プレーヤ 4 へのオーディオデータの書き込み処理が終了する。なお、ここでは、図 4 のトラックデータファイル 1010 ～ 1013 についてのみ述べたが、携帯用プレーヤ 4 は、図 4 の再生管理ファイルについても同様に適宜更新を行う。

【0136】携帯用記憶装置 3 からの読み出し動作
 図 25 は、携帯用記憶装置 3 から携帯用プレーヤ 4 への読み出し動作を説明するためのフローチャートである。

【0137】ステップ S 61：携帯用プレーヤ 4 から携帯用記憶装置 3 に、読み出しを要求するトラックデータ (曲) を特定した読み出し要求信号が出力される。

【0138】ステップ S 2：図 21 を用いて前述したように、携帯用記憶装置 3 と携帯用プレーヤ 4 との間で相互認証処理を行う際に用いる認証鍵データ IK_j の選択処理が行われる。

【0139】ステップ S 3：図 22 を用いて前述したように、携帯用記憶装置 3 と携帯用プレーヤ 4 との間で相互認証処理が行われる。

【0140】ステップ S 4：ステップ S 3 の相互認証処理によって携帯用記憶装置 3 および携帯用プレーヤ 4 の双方が相手を正当であると認めた場合には、ステップ S 5 の処理が行われ、そうでない場合には処理が終了する。

【0141】ステップS5：携帯用記憶装置3および携帯用プレーヤ4において、セッション鍵データS e kが生成される。

【0142】ステップS63：暗号化されたオーディオデータを、通信インターフェイス32、42を介して、携帯用記憶装置3から携帯用プレーヤ4に読み出す。当該処理については後述する。

【0143】すなわち、オーディオシステム1では、携帯用記憶装置3と携帯用プレーヤ4との間で相互認証が行われ、双方が相手を正当であると認めた場合にのみ、後述するように、携帯用プレーヤ4において、携帯用記憶装置3から携帯用プレーヤ4に出力された暗号化されたコンテンツ鍵データCKを適切なセッション鍵データS e kで解読できる。そのため、著作権侵害を招くようなオーディオデータの不正な利用が容易に行われることを回避できる。

【0144】〔携帯用記憶装置3からのオーディオデータの読み出し処理（図25に示すステップS63）〕図26は、携帯用記憶装置3から携帯用プレーヤ4へのオーディオデータの読み出し処理を説明するための図である。なお、当該読み出し処理は、前述した図20に示す書き込み処理の後に行われるため、図4に示すトラックデータファイル1010～1013には、図10に示すように、T R I N Fにコンテンツ鍵データCKが設定され、パーツ毎にパーツ鍵データPKが設定され、各クラスC L内にはブロックシードデータB Sが設定されている。また、ステップS5の処理が終了しているため、携帯用記憶装置3および携帯用プレーヤ4は、正当な相手同士であれば、同じセッション鍵データS e kを有している。

【0145】ステップS71：携帯用記憶装置3は、フラッシュメモリ34に記憶されている図4に示すトラックデータファイル1010～1013のうち読み出し要求信号で特定されるトラックデータに対応するトラック

$$TMK = PK \text{ XOR } CK$$

ステップS78：携帯用プレーヤ4の鍵生成／鍵演算ユニット62において、ステップS76で生成したテンポラリ鍵データTMKと、ステップS71で入力されたトラックデータファイルのクラス内の図10に示すブロックシードデータB Sとを用いて、下記式（14）に示

$$BK = MAC (TMK, BS)$$

ステップS79：携帯用プレーヤ4は、暗号化／復号ユニット64において、ステップS78で生成したブロック鍵データBKを用いて、ステップS71で入力したオーディオデータを復号する。このとき、オーディオデータの復号は、各ブロック毎に、それぞれ個別に求められたブロック鍵データBKを用いて行われる。また、復号は、暗号化の単位である8バイトのブロックを単位として行われる。

【0154】ステップS80：携帯用プレーヤ4は、圧

データファイルを特定し、当該特定したトラックデータファイルを構成するクラス内のオーディオデータを、サウンドユニットS Uを単位として読み出して携帯用プレーヤ4に出力する。携帯用記憶装置3は、また、上記トラックデータファイルの属性ヘッダを読み出して携帯用プレーヤ4に出力する。

【0146】ステップS72：携帯用プレーヤ4は、当該入力された属性ヘッダのうち、T R I N Fから暗号化されたコンテンツ鍵CKを抽出し、携帯用記憶装置3に出力する。

【0147】ステップS73：携帯用記憶装置3の暗号化／復号ユニット54は、ステップS72で入力されたコンテンツ鍵データCKを、記憶ユニット51に記憶されている記憶用鍵データS K_mを用いて復号する。

【0148】ステップS74：携帯用記憶装置3の暗号化／復号ユニット54は、ステップS73で復号したコンテンツ鍵データCKを、図25に示すステップS5で得られたセッション鍵データS e kを用いて暗号化する。

【0149】ステップS75：携帯用記憶装置3は、ステップS74で暗号化したコンテンツ鍵データCKを携帯用プレーヤ4に出力する。

【0150】ステップS76：携帯用プレーヤ4の暗号化／復号ユニット64は、ステップS73で携帯用記憶装置3から入力したコンテンツ鍵データCKを、セッション鍵データS e kを用いて復号する。

【0151】ステップS77：携帯用プレーヤ4の鍵生成／演算ユニット62は、ステップS76で復号されたコンテンツ鍵データCKと、ステップS71で入力された属性ヘッダの中のP R T I N Fに含まれるパーツ鍵データPKとの排他的論理和を演算し、当該演算結果をテンポラリ鍵データTMKとする。

【0152】

【数13】

・・・（13）

すMAC演算を行い、当該演算結果をブロック鍵データBKとする。ブロック鍵データBKは、ブロック毎に求められる。

【0153】

【数14】

・・・（14）

縮／伸長モジュール45において、ステップS79で復号したオーディオデータをA T R A C 3方式で伸長し、当該伸長したオーディオデータを、D/A変換器47でデジタル形式に変換した後に、スピーカ46に出力する。このとき、圧縮／伸長モジュール45は、ステップS78で復号したオーディオデータを、サウンドユニットS Uを単位として伸長する。以上の処理によって、携帯用記憶装置3から携帯用プレーヤ44へのオーディオデータの読み出しおよび再生が終了する。

【0155】〔トラックデータファイルの分割編集処理〕前述したように、携帯用プレーヤ4の編集モジュール44は、1個のトラックデータファイルを分割して2個のトラックデータファイルを生成する分割編集処理と、2個のトラックデータファイルを結合して1個のトラックデータファイルを生成する結合編集処理とを行う。

【0156】まず、分割編集処理について説明する。図27は、携帯用プレーヤ4の編集モジュール44によるトラックデータファイルの分割編集処理を説明するための図である。編集モジュール44は、例えば、図27Aに示す1個のトラックデータファイル(1)を、図27Bに示すトラックデータファイル(1)と、図27Cに示すトラックデータファイル(2)とに分割する。このとき、分割の区切りとなる最小単位はサウンドユニットSUであり、当該例では、図27Bに示すように、トラックデータファイル(1)のクラスタCL(2)のサウンドユニットSU(3)とSU(4)との間で分割されている。

【0157】当該分割により、分割後のトラックデータファイル(1)のクラスタCL(2)は図28Aに示すようになり、新たに生成されたトラックデータファイル(2)のクラスタCL(0)は図28Bに示すようになる。このとき、図28Bに示すように、トラックデータファイル(2)のクラスタCL(0)のサウンドユニットSU(0)は分割前のトラックデータファイル(1)のクラスタ(2)のサウンドユニットSU(4)となり、トラックデータファイル(2)のクラスタCL(0)のサウンドユニットSU(1)は分割前のトラックデータファイル(1)のクラスタ(2)のサウンドユニットSU(5)となる。また、図28Bに示すトラックデータファイル(2)のクラスタCL(0)のブロック暗号化初期値IVには、図27A、Bに示すトラックデータファイル(1)のクラスタCL(2)内のサウンドユニットSU(3)の最後の8バイトが設定される。

【0158】本実施形態では、前述したように各クラスタ内において、最初のサウンドユニットSU(0)の直前にブロック暗号化初期値IVを配置したことで、分割の際に、分割位置の直前の8バイトをそのままブロック暗号化初期値IVとして用いれば良く、新たなトラックデータファイルを作成する際の処理を簡単にできる。また、再生時に、サウンドユニットSU(0)と共に、そ

$$PK_2 = CK_1 \text{ XOR } PK_1 \text{ XOR } CK_2$$

これにより、トラックデータファイル(2)について、前記式(11)に基づいてされるテンポラリ鍵データは、トラックデータファイル(1)のテンポラリ鍵データと同じになり、前記式(12)に基づいて生成されるブロック鍵データも分割前のブロック鍵データBK_1と同じにできる。そのため、トラックデータファイル

の直前のブロック暗号化初期値IVを読み出せばよいため、再生処理も簡単になる。

【0159】本実施形態では、分割前のトラックデータファイル(1)のコンテンツ鍵データ、パーツ鍵データおよびブロック鍵データは、それぞれCK_1、PK_1およびBK_1である。また、分割後のトラックデータファイル(1)のコンテンツ鍵データ、パーツ鍵データおよびブロック鍵データは、それぞれCK_1'、PK_1'およびBK_1である。また、トラックデータファイル(2)のコンテンツ鍵データ、パーツ鍵データおよびブロック鍵データは、それぞれCK_2、PK_2およびBK_1である。

【0160】図29は、携帯用プレーヤ4の編集モジュール44において、新たなトラックデータファイル(2)のコンテンツ鍵データおよびパーツ鍵データを生成する方法を説明するための図である。分割により生成された新たなトラックデータファイル(2)は、トラックデータファイル(1)とは別に新たなコンテンツ鍵データCK_2を有する。本実施形態では、パーツ鍵データPK_2を以下に示すように算出することで、ブロック鍵データBK_1を分割前と同じにする。

【0161】ステップS90：編集モジュール44は、トラックデータファイルの分割指示を入力したか否かを判断し、入力したと判断した場合にはステップS91の処理を実行し、入力していないと判断した場合にはステップS90の処理を繰り返す。

【0162】ステップS91：編集モジュール44は、乱数発生ユニット60に乱数を発生させ、当該乱数に応じたコンテンツ鍵データCK_2を新たに生成する。

【0163】ステップS92：携帯用記憶装置3の暗号化／復号ユニット54において、ステップS91で生成したコンテンツ鍵データCK_2を、記憶ユニット51に記憶されている記憶用鍵データSKmを用いて暗号化する。

【0164】ステップS93：編集モジュール44は、当該暗号化されたコンテンツ鍵データCK_2を、当該トラックデータファイルのTRKINFに書き込む。

【0165】ステップS94：編集モジュール44は、トラックデータファイル(2)のパーツ鍵データPK_2を下記式(15)に基づいて生成する。

【0166】

【数15】

$$\dots (15)$$

(2)内のサウンドユニットSUを新たなブロック鍵データを用いて再度暗号化する必要がない。

【0167】ステップS95：編集モジュール44は、ステップS94で生成したパーツ鍵データPK_2を、当該トラックデータファイルPRINFにそのまま書き込む。

【0168】このように、オーディオシステム1では、分割して新たに生成したトラックデータファイル(2)のコンテンツ鍵データとして、新たなコンテンツ鍵データCK__2を用いた場合でも、上記式(15)に基づいてパーツ鍵データPK__2を生成することで、テンポラリ鍵データを分割前のテンポラリ鍵データと同じにできる。その結果、ブロック鍵データも分割前のブロック鍵データBK__1と同じにでき、トラックデータファイル(2)内のサウンドユニットSUを新たなブロック鍵データを用いて再度暗号化する必要がない。また、同様に、分割後のトラックデータファイル(1)のパーツ鍵データPK__1'も、ブロック鍵データBK__1を変えないように、コンテンツ鍵データCK__1'に応じた決定される。その結果、分割後のトラックデータファイル(1)内のサウンドユニットSUを新たなブロック鍵データを用いて再度暗号化する必要もない。そのため、トラックデータファイルの分割編集に伴い演算量が大幅に増加することを回避できる。なお、ここでは、図4のトラックデータファイルについてのみ述べたが、編集モジュール44は、図4の再生管理ファイル100についても同様に適宜更新を行う。

【0169】次に、トラックデータファイルの結合編集処理について説明する。図30は、携帯用プレーヤ4の編集モジュール44によるトラックデータファイルの結合編集処理を説明するための図である。図30に示すように、編集モジュール44は、例えば、図30Aに示すトラックデータファイル(1)と、図30Bに示すトラックデータファイル(2)とを結合して、図30Cに示すトラックデータファイル(3)を生成する。

【0170】当該結合により、結合前のトラックデータファイル(1)からなるパーツ(1)と、結合前のトラックデータファイル(2)からなるパーツ(2)を含む新たなトラックデータファイル(3)が生成される。また、トラックデータファイル(3)のコンテンツ鍵データとして新たなコンテンツ鍵データCK__3が生成され、パーツ(1)のパーツ鍵データPK__3__1およびパーツ(2)のパーツ鍵データPK__3__2が後述するようにして新たに生成される。また、当該トラックデータファイル(3)のTRKINFおよびPRTINFに、新たに生成された鍵データが後述するように設定される。

【0171】また、パーツ(1)の図6に示すPRTSIZEが示す開始クラスタおよび終了クラスタとして、結合前のトラックデータファイル(1)のクラスタCL

$$PK_3_1 = CK_1 \text{ XOR } PK_1 \text{ XOR } CK_3$$

これにより、前記式(11)に基づいて生成されるパーツ(1)のテンポラリ鍵データを結合前のトラックデータファイル(1)のテンポラリ鍵データと同じにでき、その結果、前記式(12)に基づいて生成されるパーツ

(0)およびCL(4)がそれぞれ設定される。また、パーツ(2)のPRTSIZEが示す開始クラスタおよび終了クラスタとして、結合前のトラックデータファイル(2)のクラスタCL(0)およびCL(5)がそれぞれ設定される。

【0172】図31は、携帯用プレーヤ4の編集モジュール44において、新たに生成したトラックデータファイル(3)のパーツ(1)および(2)のパーツ鍵データを生成する処理を説明するための図である。なお、本実施形態では、結合の対象となるトラックデータファイル(1)がコンテンツ鍵データCK__1、パーツ鍵データPK__1およびブロック鍵データBK__1を用いており、トラックデータファイル(2)がコンテンツ鍵データCK__2、パーツ鍵データPK__2およびブロック鍵データBK__2を用いてる場合を例示して説明する。

【0173】ここで、トラックデータファイル(3)は新たなコンテンツ鍵データCK__3を得るが、パーツ(1)および(2)のパーツ鍵データを以下に示すように算出することで、各ブロックのブロック鍵データBK__1およびBK__2を結合前と同じにできる。

【0174】ステップS100：編集モジュール44は、トラックデータファイルの結合指示を入力したか否かを判断し、入力したと判断した場合にはステップS101の処理を実行し、入力していないと判断した場合にはステップS100の処理を繰り返す。

【0175】ステップS101：編集モジュール44は、乱数発生ユニット60に乱数を発生させ、当該乱数に応じたコンテンツ鍵データCK__3を新たに生成する。

【0176】ステップS102：携帯用記憶装置3の暗号化／復号ユニット54において、ステップS101で生成したコンテンツ鍵データCK__3を、記憶ユニット51に記憶されている記憶用鍵データSKmを用いて暗号化する。

【0177】ステップS103：編集モジュール44は、当該暗号化されたコンテンツ鍵データCK__3を当該トラックデータファイルのTRKINFに書き込む。

【0178】ステップS104：編集モジュール44は、トラックデータファイル(3)のパーツ(1)のパーツ鍵データPK__3__1を下記式(16)に基づいて生成する。

【0179】

【数16】

$$\dots (16)$$

(1)のブロック鍵データも結合前のトラックデータファイル(1)のブロック鍵データBK__1と同じにできる。そのため、パーツ(1)のサウンドユニットSUを新たなブロック鍵データを用いて再度暗号化する必要が

ない。

【0180】ステップS105：編集モジュール44は、トラックデータファイル(3)のパーツ(2)のパーツ鍵データPK__3__2を下記式(17)に基づいて

$$PK_3_2 = CK_2 \text{ XOR } PK_2 \text{ XOR } CK_3$$

これにより、前記式(11)に基づいて生成されるパーツ(2)のテンポラリ鍵データを結合前のトラックデータファイル(2)のテンポラリ鍵データと同じにでき、その結果、前記式(12)に基づいて生成されるパーツ(2)のブロック鍵データも結合前のトラックデータファイル(2)のブロック鍵データBK__2と同じにできる。そのため、パーツ(2)のサウンドユニットSUを新たなブロック鍵データを用いて再度暗号化する必要がない。

【0182】ステップS106：編集モジュール44は、ステップS104で生成したパーツ鍵データPK__3__1をトラックデータファイル(3)のパーツ(1)のPRTINFにそのまま書き込む。

【0183】ステップS107：編集モジュール44は、ステップS105で生成したパーツ鍵データPK__3__2をトラックデータファイル(3)のパーツ(2)のPRTINFにそのまま書き込む。

【0184】このように、オーディオシステム1では、結合して新たに生成したトラックデータファイル(3)のコンテンツ鍵データとして、新たなコンテンツ鍵データCK__3を用いた場合でも、上記式(16)および(17)に基づいてパーツ鍵データPK__3__1およびPK__3__2を生成することで、各パーツのテンポラリ鍵データを結合前と同じにできる。その結果、各パーツのブロック鍵データも結合前のブロック鍵データBK__1およびBK__2とそれぞれ同じにでき、パーツ(1)および(2)内のサウンドユニットSUを新たなブロック鍵データを用いて再度暗号化する必要がない。そのため、トラックデータファイルの結合編集に伴い演算量が大幅に増加することを回避できる。なお、ここでは、図4のトラックデータファイルについてのみ述べたが、編集モジュール44は、図4の再生管理ファイルについても同様に適宜更新を行う。

【0185】この発明は、上述した実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えば、上述した実施形態では、ATRAC3方式の圧縮の単位であるサウンドユニットSUのバイト数(160バイト)が、CBCモードの暗号化の単位である暗号化ブロックのバイト数(8バイト)の整数倍になる場合を例示したが、この発明は、例えば、整数倍にならない場合には、サウンドユニットSUにデータ長調整用のデータであるパディング(padding)を挿入して調整するようにしてもよい。

【0186】また、上述した実施形態では、携帯用記憶

生成する。

【0181】

【数17】

・・・(17)

装置3と携帯用プレーヤ4との間で相互認証処理を行う場合に、図22に示すように、先ず始めに携帯用記憶装置3で生成した乱数R₁を携帯用プレーヤ4に出力する場合を例示したが、先ず始めに携帯用プレーヤ4で生成した乱数を携帯用記憶装置3に出力するようにしてもよい。

【0187】また、上述した実施形態では、図21に示すように、記憶ユニット51および61に32組の認証鍵データおよびマスター鍵データを記憶した場合を例示したが、これらの組の数は2以上であれば任意である。

【0188】また、上述した実施形態では、図21に示すように、携帯用プレーヤ4において、マスター鍵データMK₁～MK₃₁から認証鍵データIK₁～IK₃₁を生成する場合を例示したが、携帯用プレーヤ4に、携帯用記憶装置3と同じように、認証鍵データIK₁～IK₃₁を記憶し、乱数R₁に応じた認証鍵データを選択するようにしてもよい。

【0189】また、上述した実施形態では、図21に示すように、携帯用記憶装置3および携帯用プレーヤ4において、携帯用プレーヤ4で生成した乱数R₁を用いて、認証鍵データIK₁およびマスター鍵データMK₁を選択する場合を例示したが、携帯用記憶装置3で生成した乱数を用いてもよいし、携帯用記憶装置3および携帯用プレーヤ4の双方で発生した乱数を用いてもよい。

【0190】また、上述した実施形態では、図21に示すように、携帯用記憶装置3および携帯用プレーヤ4において乱数R₁に基づいて認証鍵データIK₁およびマスター鍵データMK₁を選択する場合を例示したが、この発明は、例えば、携帯用記憶装置3および携帯用プレーヤ4に外部から5ビットの鍵選択指示データを入力し、当該鍵選択指示データで指示される相互に対応する認証鍵データIK₁およびマスター鍵データMK₁を、携帯用記憶装置3および携帯用プレーヤ4で選択してもよい。

【0191】また、上述した実施形態では、トラックデータとしてオーディオデータを含むデータを例示したが、この発明は、その他、動画像データ、静止画像データ、文書データおよびプログラムデータなどを含むトラックデータをフラッシュメモリ34に記憶する場合にも適用できる。

【0192】

【発明の効果】以上説明したように、この発明のデータ処理システムおよびその方法によれば、記憶手段に記憶された暗号化されたデータを、所定の処理ブロックを単

位として効率的に処理できる。

【図面の簡単な説明】

【図 1】この発明の一実施形態のオーディオシステムのシステム構成を示すブロック図である。

【図 2】携帯用記憶装置および携帯用プレーヤの内部構成を示すブロック図である。

【図 3】携帯用記憶装置内の記憶ユニットに記憶されているデータを説明するための略線図である。

【図 4】携帯用記憶装置のフラッシュメモリに記憶されるデータを説明するための略線図である。

【図 5】再生管理ファイルのデータ構成を概略的に示す略線図である。

【図 6】データファイルのデータ構成を概略的に示す略線図である。

【図 7】再生管理ファイルのデータ構成をより詳細に示す略線図である。

【図 8】再生管理ファイルの各部分と付加情報領域の構成を示す略線図である。

【図 9】携帯用プレーヤの記憶ユニットに記憶されているデータを説明するための略線図である。

【図 1 0】データファイルのデータ構成をより詳細に示す略線図である。

【図 1 1】データファイルの属性ヘッダの一部を示す略線図である。

【図 1 2】データファイルの属性ヘッダの一部を示す略線図である。

【図 1 3】録音モードの種類と、各録音モードにおける録音時間等を示す略線図である。

【図 1 4】コピー制御情報を説明するための略線図である。

【図 1 5】データファイルの属性ヘッダの一部を示す略線図である。

【図 1 6】データファイルの各データブロックのヘッダを示す略線図である。

【図 1 7】携帯用プレーヤの記憶ユニットに記憶されているデータを説明するための略線図である。

【図 1 8】携帯用プレーヤの暗号化／復号ユニットの C B C モードにおける暗号化処理を説明するための略線図である。

【図 1 9】携帯用プレーヤの暗号化／復号ユニットの C B C モードにおける復号処理を説明するための略線図である。

【図 2 0】携帯用プレーヤから携帯用記憶装置への書き

込み動作を説明するためのフローチャートである。

【図 2 1】相互認証ユニットによる認証鍵データ I K_i の選択処理を説明するための略線図である。

【図 2 2】携帯用記憶装置と携帯用プレーヤとの間の相互認証処理を説明するためのフローチャートである。

【図 2 3】セッション鍵データ S e k の生成処理を説明するための略線図である。

【図 2 4】携帯用プレーヤから携帯用記憶装置へのオーディオデータの書き込み処理を説明するためのフローチャートである。

【図 2 5】携帯用記憶装置から携帯用プレーヤへの読み出し動作を説明するためのフローチャートである。

【図 2 6】携帯用記憶装置から携帯用プレーヤへのオーディオデータの読み出し処理を説明するためのフローチャートである。

【図 2 7】携帯用プレーヤの編集モジュールによるトラックデータファイルの分割編集処理を説明するための略線図である。

【図 2 8】分割編集処理を行った後のクラスタ内のデータを説明するための略線図である。

【図 2 9】携帯用プレーヤの編集モジュールにおいて、分割編集時に、新たなトラックデータファイルのコンテンツ鍵データおよびパーツ鍵データを生成する方法を説明するためのフローチャートである。

【図 3 0】携帯用プレーヤの編集モジュールによるトラックデータファイルの結合編集処理を説明するための略線図である。

【図 3 1】携帯用プレーヤ 4 の編集モジュールにおいて、新たに生成したトラックデータファイル (3) のパーツ (1) および (2) のパーツ鍵データを生成する処理を説明するための略線図である。

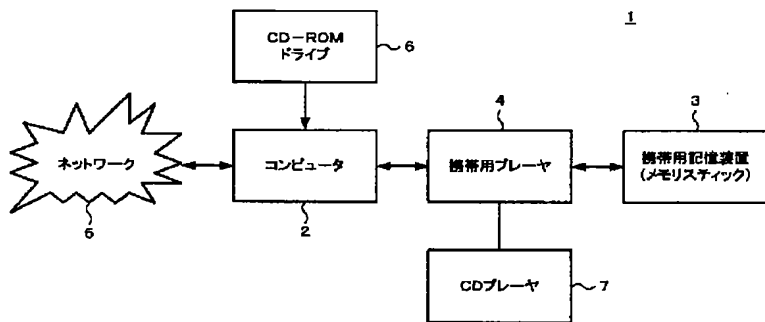
【符号の説明】

1・・・オーディオシステム、2・・・コンピュータ、3・・・携帯用記憶装置、4・・・携帯用プレーヤ、5・・・ネットワーク、3 3、4 3・・・制御モジュール、5 0、6 0・・・乱数発生ユニット、5 1、6 1・・・記憶ユニット、5 2、6 2・・・鍵生成／演算ユニット、5 3、6 3・・・相互認証ユニット、5 4、7 4・・・暗号化／復号ユニット、5 5、6 5・・・制御ユニット、3 4・・・フラッシュメモリ、4 4・・・編集モジュール、4 5・・・圧縮／伸長モジュール、4 6・・・スピーカ

【図 1 5】

0x0370	PRTSIZE	PRTKEY	Reserved(8)
0x0380	CONNUM0	PRTSIZE(0x0388)	PRTKEY
0x0390		Reserved(8)	CONNUM0

【図 1】

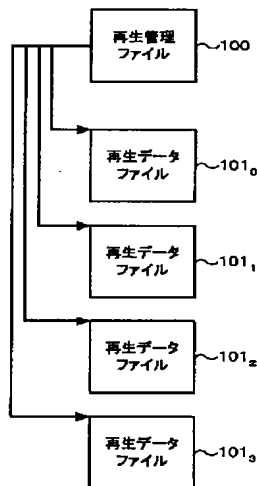


【図 3】

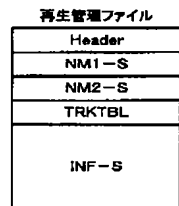
携帯用記憶装置3の記憶ユニット51に記憶されるデータ

隠証鍵子一タ IK_0
 IK_1
 IK_2
 IK_3
 \vdots
 IK_{30}
 IK_{31}
 装置識別子一タ ID_0
 記憶用鍵子一タ SK_m

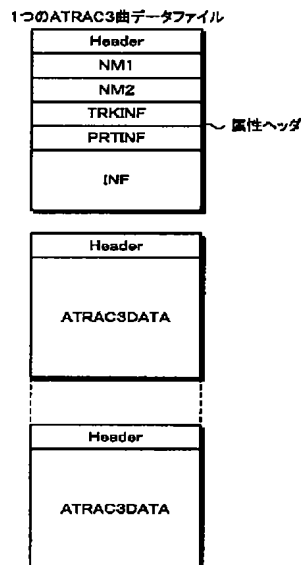
【図 4】



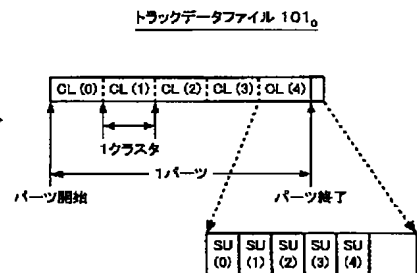
【図 5】



【図 6】



【図 9】



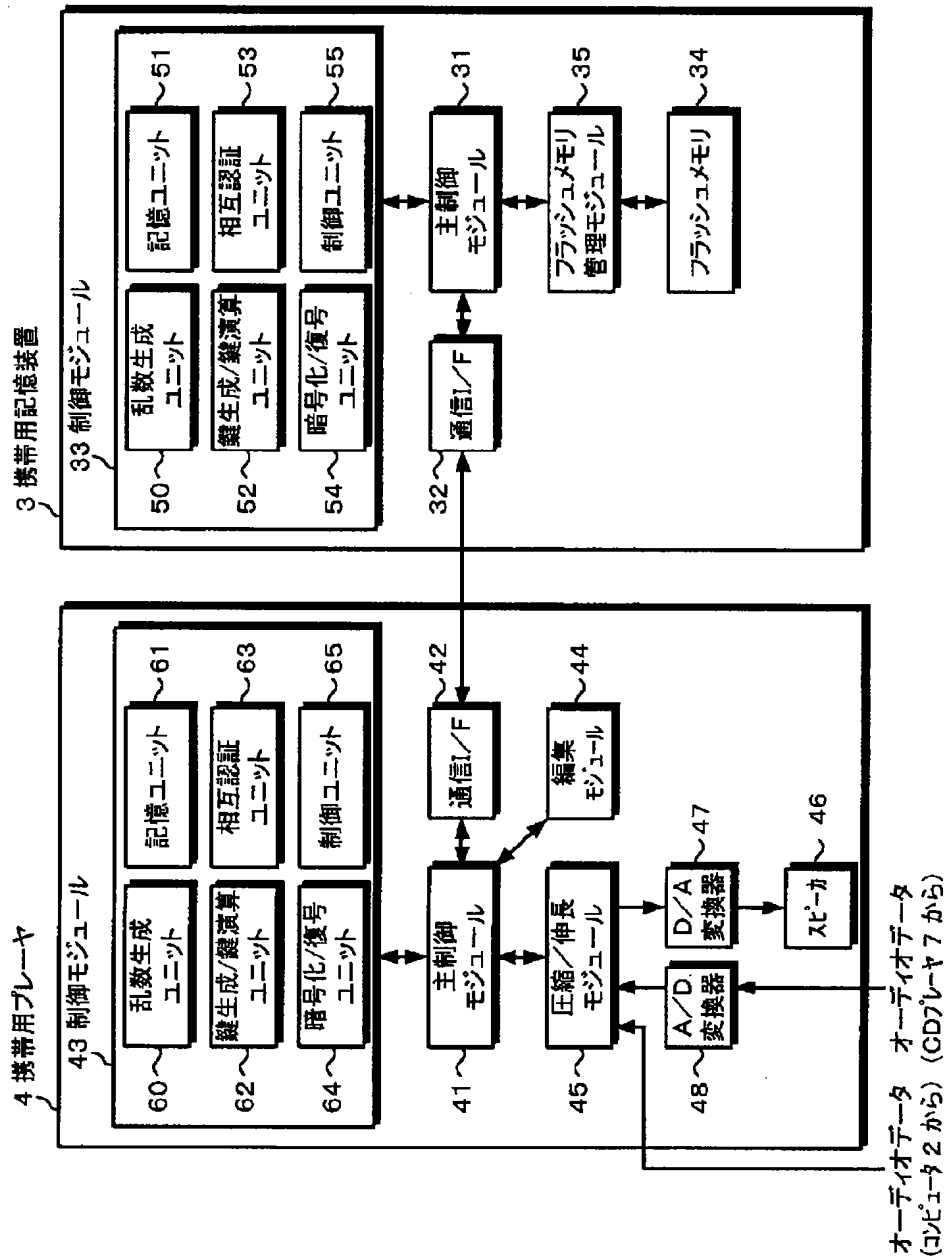
携帯用記憶装置3のフラッシュメモリ34の記憶データ

【図 7】

再生管理ファイル(PBLIST)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID-TL0				Reserved		MCode		REVISION				Reserved			
0x0010	SN1C+L		SN2C+L		SINFSIZE		T-TRK		VerNo		Reserved					
0x0020	NM1-S(256)															
0x0120	NM2-S(512)															
0x0320	Reserved								CONTENTSKEY							
0x0330	Reserved								MAC							
	Reserved															
													S-YMDhms			
0x0360	TRK-001		TRK-002		TRK-003		TRK-004		TRK-005		TRK-006		TRK-007		TRK-008	
	TRK-009		TRK-010		TRK-011		TRK-012		TRK-013		TRK-014		TRK-015		TRK-016	
0x0660	TRK-393		TRK-394		TRK-395		TRK-396		TRK-397		TRK-398		TRK-399		TRK-400	
0x0647	JNF-S(14720)															
0x3FF0	BLKID-TL0				Reserved		MCode		REVISION				Reserved			

【図2】



【図8】

A

0x0000	BLKID-TL0				Reserved	MCode	REVISION				Reserved				
0x0010	SN1C+L		SN2C+L		SINFSIZE	T-TRK		VerNo		Reserved					

B

0x0020	NM1-S(256)															
0x0120	NM2-S(512)															
0x0320	Reserved								CONTENTSKEY							
0x0330	Reserved								MAC							
	Reserved												S-YMDhms			
0x0350	TRK-001	TRK-002	TRK-003	TRK-004	TRK-005	TRK-006	TRK-007	TRK-008	TRK-009	TRK-010	TRK-011	TRK-012	TRK-013	TRK-014	TRK-015	TRK-016
0x0360	TRK-017	TRK-018	TRK-019	TRK-020	TRK-021	TRK-022	TRK-023	TRK-024	TRK-025	TRK-026	TRK-027	TRK-028	TRK-029	TRK-030	TRK-031	TRK-032
0x0680	TRK-393	TRK-394	TRK-395	TRK-396	TRK-397	TRK-398	TRK-399	TRK-400								
0x0670	INF-S(14720)															
0x3FF0	BLKID-TL0				Reserved	MCode	REVISION				Reserved					

C

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	INF	0x00	ID	0x00	SIZE	MCode		C+L		Reserved		DATA 可変長				

【図11】

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID-HD0				Reserved		MCode		Reserved				BLOCK SERIAL			
0x0010	N1C+L		N2C+L		INFSIZE		T-PRT		T-SU				INX		XT	
0x0020	NM1(256)															
0x0120	NM2(512)															
0x0310																

【図12】

0x0320	Reserved(8)				CONTENTSKEY							
	Reserved(8)				MAC							
	Reserved(12)						A	LT	FN0			
	MG(D)SERIAL-nnn											
0x0360	CONNUM		YMDhms-S		YMDhms-E		MT	CT	CC	CN		

【図14】

bit7	コピー許可	0:コピー禁止	1:コピー可
bit6	世代	0:オリジナル	1:第1世代以上
HCMS bit5-4	高速デジタルコピーに関するコピー制御		
	00:コピー禁止	01:コピー第1世代	10:コピー可
	コピー第1世代のコピーした子供はコピー禁止とする。		
bit3-2	MagicGate認証レベル		
	00:Level10(Non-MG)	01:Level1	
	10:Level2	11:Reserved	
	Level10以外はデバインド、コンバイン出来ません。		
bit1,0	Reserved		

【図 10】

A3Dnnnnnn.MSA(ATRAC3データファイル)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F																
0x0000	BLKID-HD0				Reserved		MCode		Reserved				BLOCK SERIAL																			
0x0010	N1C+L		N2C+L		INFSIZE		T-PRT		T-SU				INX		XT																	
0x0020	NM1(256)																															
0x0120	NM2(512)																															
0x0310																																
0x0320																	Reserved(8)								CONTENTSKEY							
																	Reserved(8)								MAC							
																	Reserved(12)												A	LT	FN0	
																	MG(D)SERIAL-nnn															
0x0360	CONNUM				YMDhms-S				YMDhms-E				MT	CT	CC	CN																
0x0370	PRTSIZE				PRTKEY								Reserved(8)																			
0x0380					CONNUM0				PRTSIZE(0x0388)				PRTKEY																			
0x0390					Reserved(8)								CONNUM0																			
	INF(0x0400)																															
0x3FFF	BLKID-HD0				Reserved		MCode		Reserved				BLOCK SERIAL																			
0x4000	BLKID-A3D				Reserved		MCode		CONNUM0				BLOCK SERIAL																			
0x4010	BLOCK SEED								INITIALIZATION VECTOR																							
0x4020	SU-000(Nbyte=384byte)																															
0x41A0	SU-001(Nbyte)																															
0x4320	SU-002(Nbyte)																															
0x04A0	SU-041(Nbyte)																															
0x7DA0	Reserved(Nbyte=208byte)																															
0x7F20	BLOCK SEED																															
0x7FF0	BLKID-A3D				Reserved		MCode		CONNUM0				BLOCK SERIAL																			

【图 16】

0x4000	BLKID-A3D	Reserved	MCode	CONNUM0	BLOCK SERIAL
0x4010	BLOCK SEED			INITIALIZATION VECTOR	
0x4020	SU-000(Nbyte=384byte)				

【図 13】

bit7: ATRAC3のモード 0: Dual 1: Joint

bit6,5,4 3bitのNはモードの値

N	モード	時間	転送レート	SU	バイト
7	HQ	47min	176kbps	31SU	512
6		58min	146kbps	38SU	424
5	EX	64min	132kbps	42SU	384
4	SP	81min	105kbps	53SU	304
3		90min	94kbps	59SU	272
2	LP	128min	66kbps	84SU	192
1	mono	181min	47kbps	119SU	136
0	mono	258min	33kbps	169SU	96

bit3: Reserved

bit2: データ区分 0: オーディオ 1: その他

bit1: 再生SKIP 0: 通常再生 1: SKIP

bit0: エンファシス 0: OFF 1: ON(50/15 μ S)

【図 17】

携帯用プレーヤ4の記憶モジュール41に記憶されるデータ

マスター鍵データ MK_0 MK_1 MK_2 MK_3

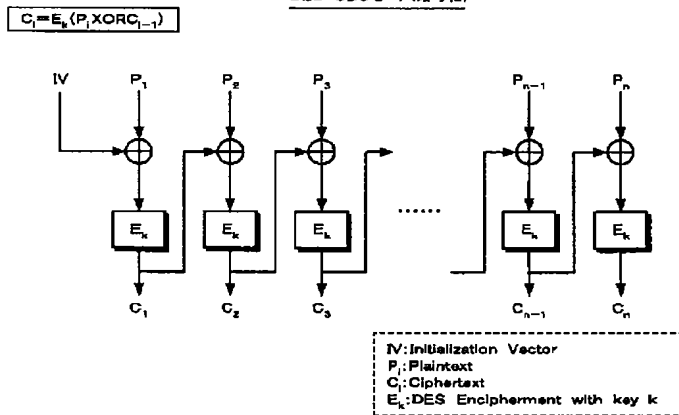
⋮

 MK_{30} MK_{31} 装置識別データ ID_d

【図 28】

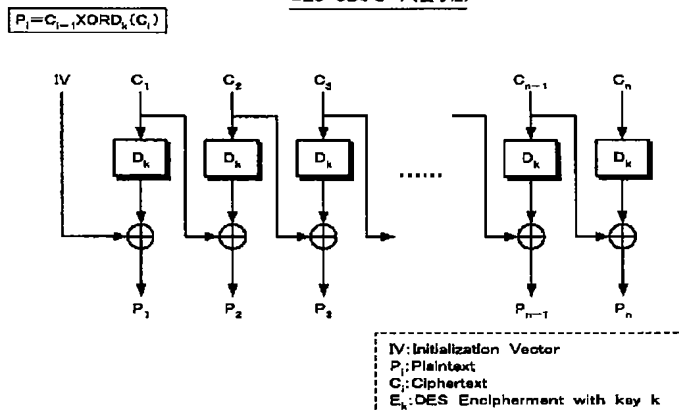
【図 18】

DES CBCモード(暗号化)

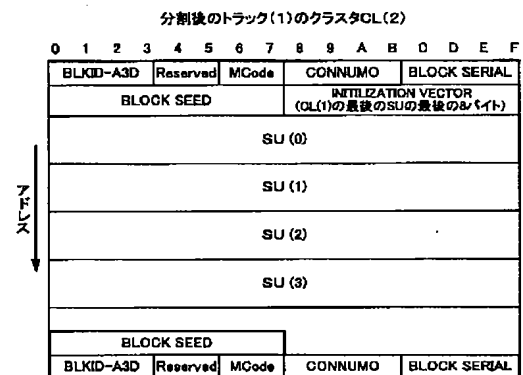


【図 19】

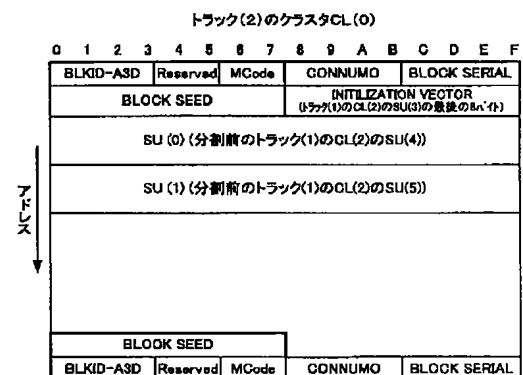
DES CBCモード(復号化)



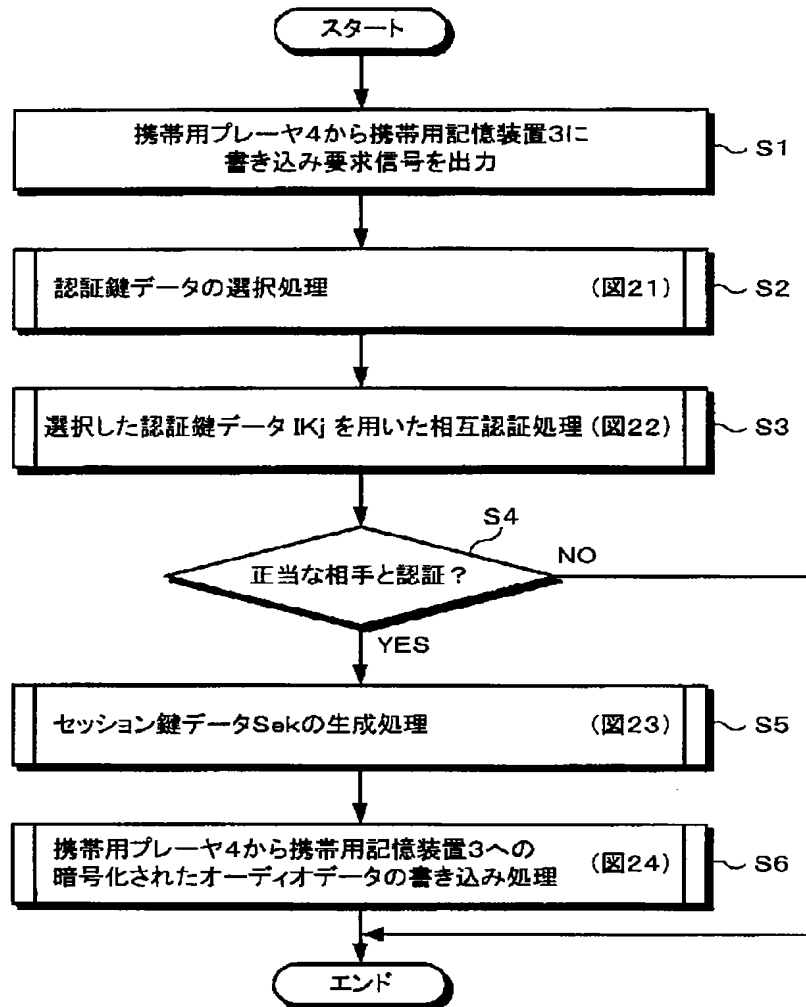
A



B

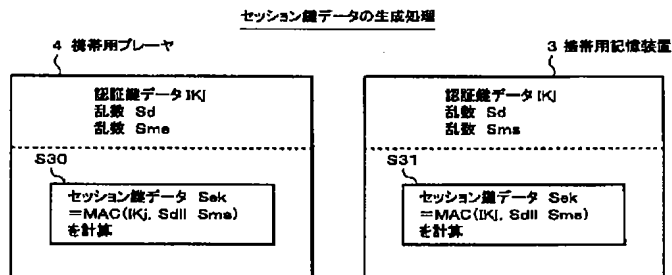


【図20】

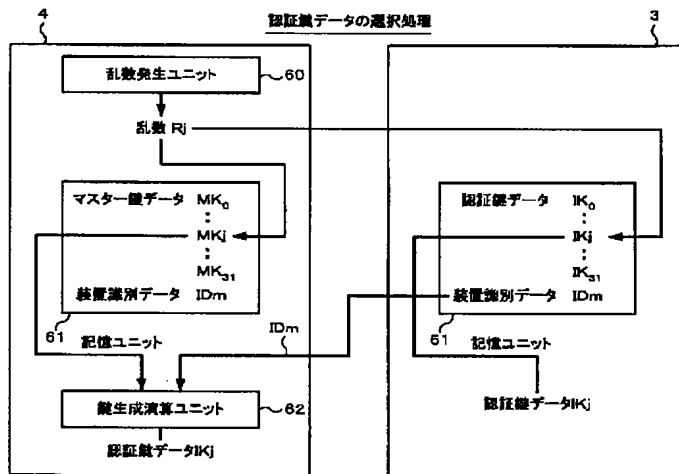


携帯用記憶装置3への書込処理

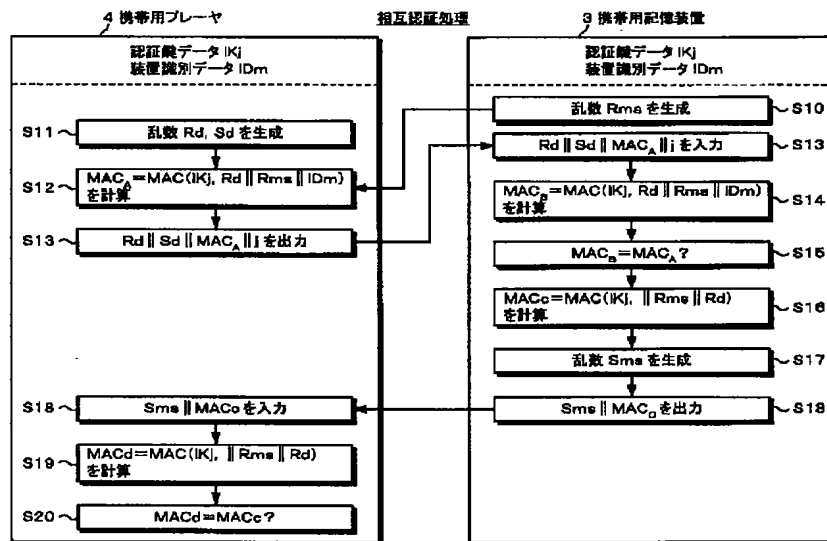
【図23】



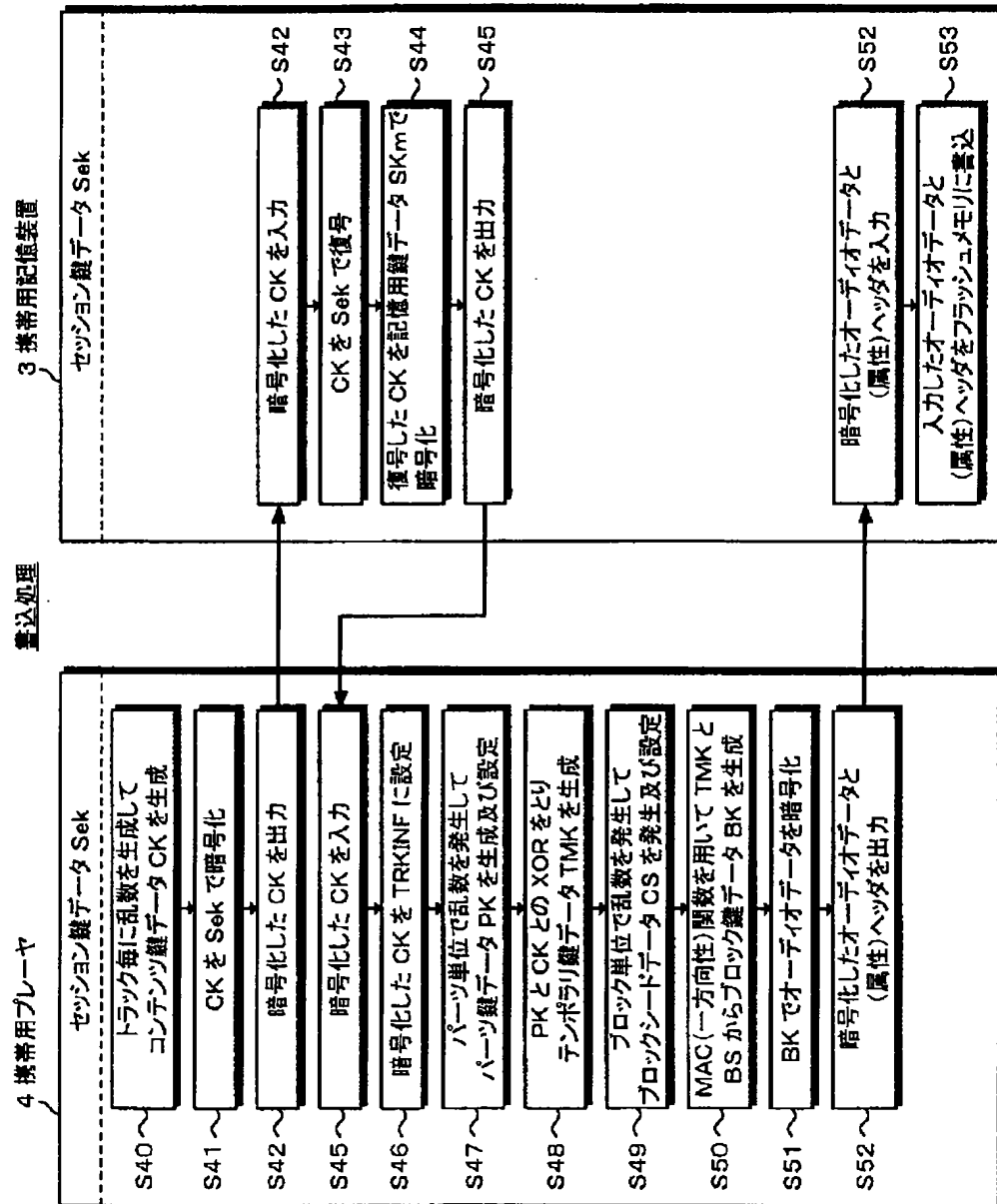
【図 21】



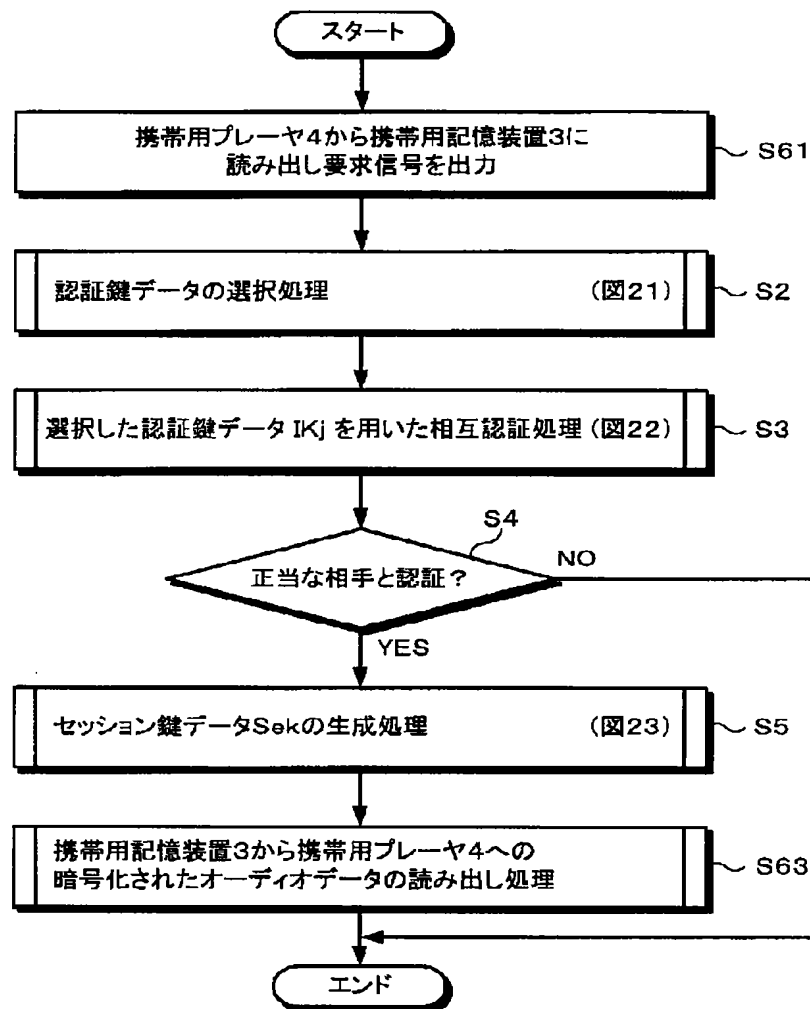
【図 22】



【図 24】

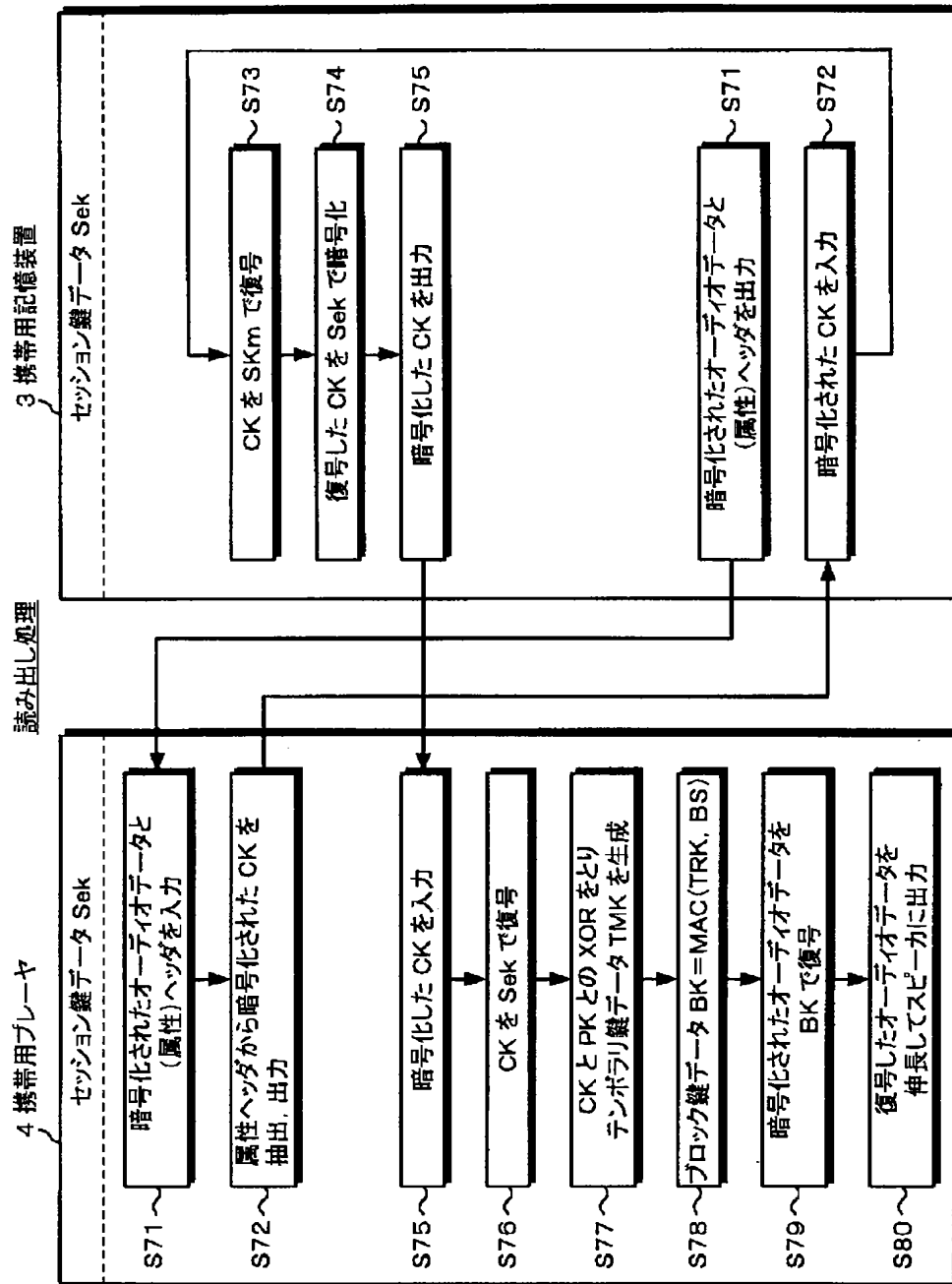


【図 25】

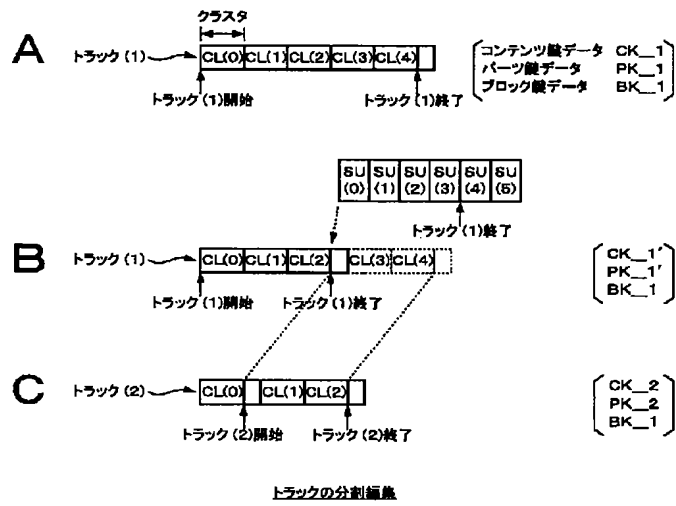


携帯用記憶装置3からの読み出し処理

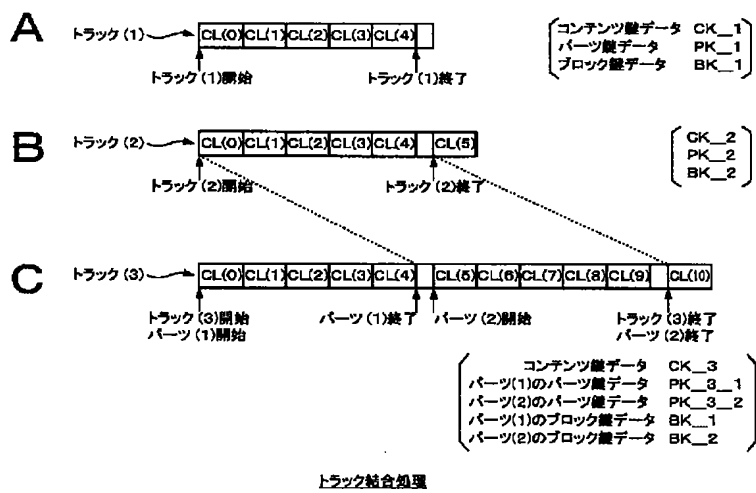
【図 26】



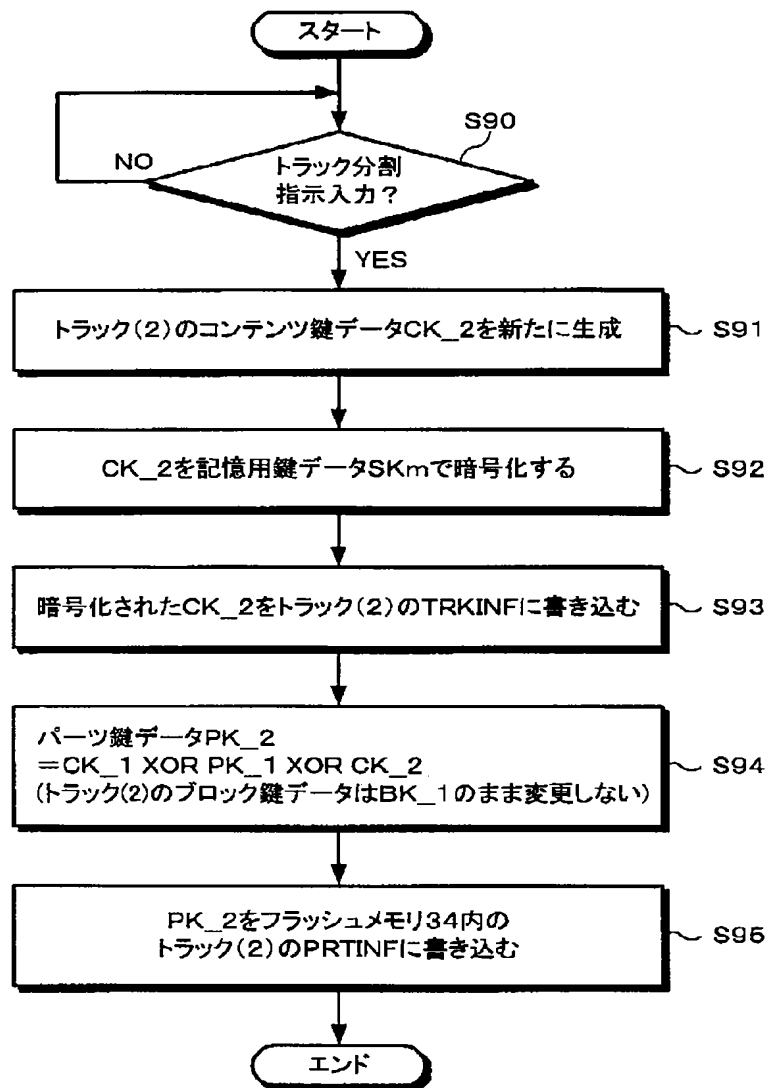
【図 27】



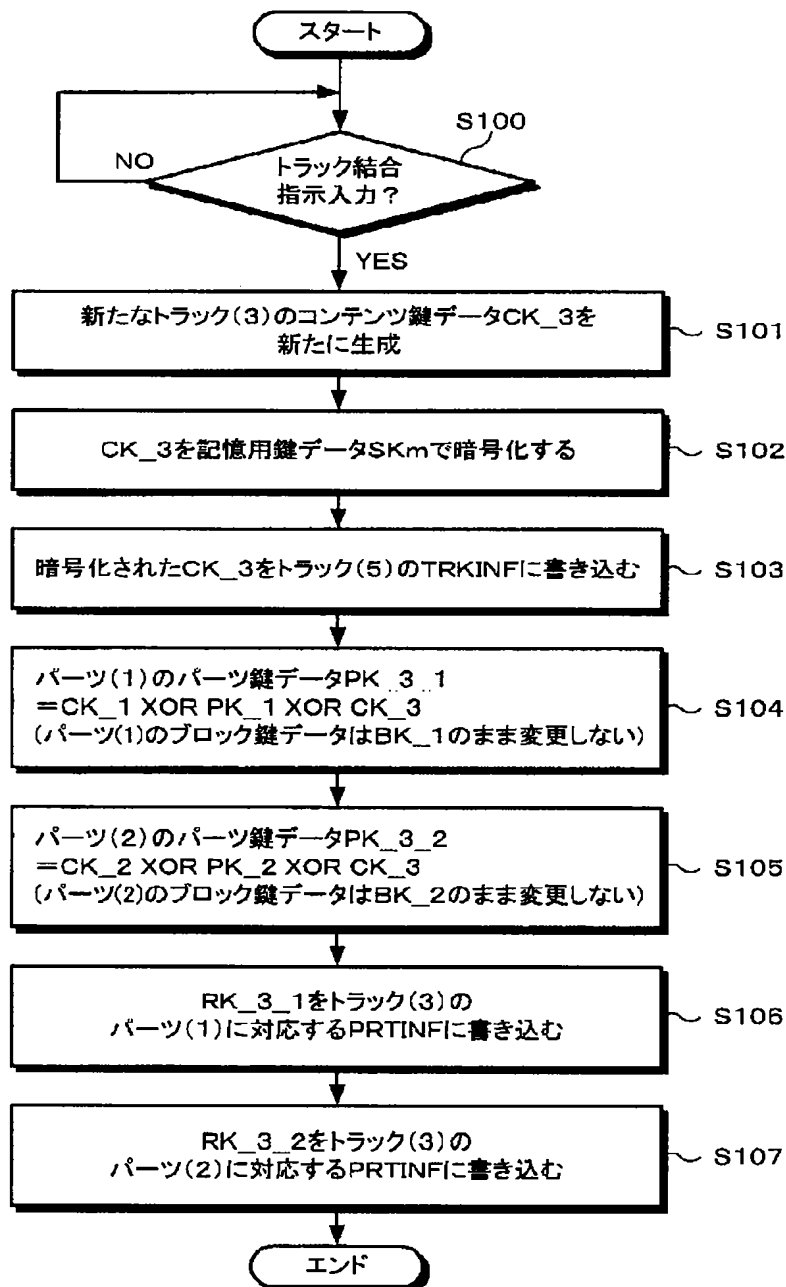
【図 30】



【図 29】



【図 31】



【手続補正書】

【提出日】平成12年4月4日（2000. 4. 4）

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0020

【補正方法】変更

【補正内容】

【0020】図5は、再生管理ファイルの構成を示し、

図6が一つ（1曲）のトラックデータファイル（以下においてATRAC3データファイルの用語がさすものもトラックデータファイルと同義である）の構成を示す。再生管理ファイルは、16KB固定長のファイルである。ATRAC3データファイルは、曲単位でもって、先頭の属性ヘッダと、それに続く実際の暗号化された音楽データとからなる。属性ヘッダも16KB固定長とさ

